TUGAS AKHIR – KS 141501

PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO/IEC 27002:2013 PADA DIREKTORAT SISTEM INFORMASI UNIVERSITAS AIRLANGGA

Stephen Christian
NRP 5211 100 075

Dosen Pembimbing 1:
Ir. Achmad Holil Noor Ali, M.Kom

Dosen Pembimbing 2:
Anisah Herdiyanti, S.Kom, M.Sc

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2015

FINAL PROJECT – KS 141501

DESIGNING AN AUDIT GUIDELINE FOR PHYSICAL AND ENVIRONMENTAL SECURITY RISK BASED AUDIT OF INFORMATION TECHNOLOGY BASED ON ISO/IEC 27002:2013 IN DIREKTORAT SISTEM INFORMASI UNIVERSITAS AIRLANGGA

Stephen Christian
NRP 5211 100 075

Supervisor 1:
Ir. Achmad Holil Noor Ali, M.Kom

Supervisor 2:
Anisah Herdiyanti, S.Kom, M.Sc

DEPARTMENT OF INFORMATION SYSTEM
Faculty of Information Technology
Institute of Technology Sepuluh Nopember
Surabaya 2015

LEMBAR PERSETUJUAN

PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO/IEC 27002:2013 PADA DIREKTORAT SISTEM INFORMASI UNIVERSITAS AIRLANGGA

TUGAS AKHIR

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

Oleh :

STEPHEN CHRISTIAN
5211 100 075

Disetujui Tim Penguji : Tanggal Ujian : 29 Juni 2015
Periode Wisuda : September 2015

Ir. Ahmad Holil Noor Ali, M.Kom. **(Pembimbing 1)**

Anisah Herdiyanti, S.Kom., M.Sc. **(Pembimbing 2)**

Feby Artwodini, S.Kom, M.T. **(Penguji 1)**

Amna Shifia Nisafani, S.Kom., M.Sc. **(Penguji 2)**

LEMBAR PENGESAHAN

PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO/IEC 27002:2013 PADA DIREKTORAT SISTEM INFORMASI UNIVERSITAS AIRLANGGA

TUGAS AKHIR

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

Oleh:

STEPHEN CHRISTIAN
5211 100 075

Surabaya, 29 Juni 2015

KETUA
JURUSAN SISTEM INFORMASI

Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom
NIP 19730219 199802 1 001

PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO/IEC 27002:2013 PADA DIREKTORAT SISTEM INFORMASI UNIVERSITAS AIRLANGGA

Nama Mahasiswa : STEPHEN CHRISTIAN
NRP : 5211 100 075
Jurusan : Sistem Informasi FTIF-ITS
Dosen Pembimbing 1 : Ir. Ahmad Holil Noor Ali, M.Kom
Dosen Pembimbing 2 : Anisah Herdiyanti, S.Kom, M.Sc

ABSTRAK

Direktorat Sistem Informasi (DSI) merupakan pusat pengembangan teknologi informasi Universitas Airlangga. Keamanan informasi merupakan salah satu hal yang perlu direncanakan dalam pengelolaan teknologi untuk menangani ancaman yang muncul. Salah satu bentuk keamanan informasi adalah keamanan fisik dan lingkungan. Untuk memastikan keamanan telah diterapkan dalam kontrolnya maka diperlukan sebuah metode yaitu audit teknologi informasi. DSI telah mengadopsi standar ISO/IEC 27001 dan 27002 sebagai standar manajemen keamanan informasi. Audit SI/TI juga telah beberapa kali dilakukan oleh pihak Direktorat Sistem Informasi Universitas Airlangga, namun pelaksanaan audit ini belum memiliki bakuan. Tidak adanya bakuan/panduan audit ini dapat menyebabkan tidak terstrukturnya proses audit yang dilakukan, seperti auditor tidak mengetahui informasi penting yang diperlukan saat audit. Berangkat dari permasalahan ini, maka dibutuhkan dokumen panduan audit teknologi informasi terutama untuk keamanan fisik dan lingkungan.

Penyusunan dokumen panduan audit teknologi informasi dimulai dengan menentukan objek penelitian melalui wawancara dengan bagian keamanan DSI. Selanjutnya dibuatlah dokumen perencanaan audit berdasarkan ruang lingkup yang sudah ditentukan. Analisis risiko aset informasi yang selanjutnya akan dipetakan dalam kontrol ISO/IEC 27002 digunakan sebagai dasar dalam penyusunan dokumen program audit.

Hasil dari tugas akhir ini adalah dokumen panduan audit yang berisi Audit Plan dan Audit Program yang berfokus pada keamanan fisik dan lingkungan TI Direktorat Sistem Informasi Universitas Airlangga yang mengacu pada ISO 27002:2013.

Kata kunci : Teknologi informasi, Audit TI, Keamanan Fisik dan Lingkungan TI, Dokumen Panduan Audit, Direktorat Sistem Informasi, ISO/IEC 27002:2013

DESIGNING AN AUDIT GUIDELINE FOR PHYSICAL AND ENVIRONMENTAL SECURITY RISK BASED AUDIT OF INFORMATION TECHNOLOGY BASED ON ISO/IEC 27002:2013 IN DIREKTORAT SISTEM INFORMASI UNIVERSITAS AIRLANGGA

Name	**: STEPHEN CHRISTIAN**
NRP	**: 5211 100 075**
Department	**: Information Systems FTIF-ITS**
Supervisor 1	**: Ir. Ahmad Holil Noor Ali, M.Kom**
Supervisor 2	**: Anisah Herdiyanti, S.Kom, M.Sc**

ABSTRACT

Direktorat Sistem Informasi (DSI) is an information technology development center in Airlangga University. Information security is one of the things that need to be planned in the management of technology to handle the emerging threats. One form of information security is the physical and environmental security. An information technology audit is a method to ensure whether the security has been applied in the existing control. DSI has adopted the standard ISO / IEC 27001 and 27002 as the standard for information security management. IS / IT Audit also has several times conducted by the Direktorat Sistem Informasi, Airlangga University, but the implementation of this audit still don't have a guideline. The absence of audit guidelines can cause to be not structured the audit process undertaken, such as the auditor does not know the necessary information during the audit. From this problem, it is necessary to make a document of the information technology audit guideliness especially for the physical and environmental security.

Preparation of information technology audit guidline begins by determining the object of research through interviews with DSI' security section. Furthermore, the audit planning documents made by the scope of which has been determined. Risk analysis of information assets will then be mapped in the control of ISO / IEC 27002 is used as the basis for preparing the document audit program..

The results of this final project is the audit guideline that contains the Audit Plan and Audit Program which focuses on IT physical and environmental security of the the Direktorat Sistem Informasi, Airlangga University based on ISO 27002:2013.

Keywords: Information technology, IT Audit, IT Physical and Environmental Security, Audit Guideline Document, the Direktorat Sistem Informasi, ISO / IEC 27002:2013

KATA PENGANTAR

Segala puji syukur dan kemuliaan penulis panjatkan kepada Tuhan Yesus Kristus karena atas limpahan kasih-Nya, kekuatan, dan pertolongan-Nya yang tidak pernah berhenti sehingga penulis dapat menyelesaikan Tugas Akhr yang berjudul "**PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO/IEC 27002:2013 PADA DIREKTORAT SISTEM INFORMASI UNIVERSITAS AIRLANGGA**" dengan tepat waktu.

Tugas Akhir ini disusun sebagai syarat kelulusan untuk menjadi sarjana komputer dari Jurusan Sistem Informasi, Institut Teknologi Sepuluh Nopember Surabaya. Penulis menyadari bahwa penyelesaian Tugas Akhir ini tidak terlepas dari bantuan dan dukungan banyak pihak. Sebab itu, penulis ingin mengucapkan terima kasih yang sangat tulus kepada:

1. David Hendrawan dan Wiwit Pujiastuti, selaku orang tua penulis yang senantiasa memberikan dukungan dalam bentuk doa dan semangat untuk menyelesaikan Tugas akhir. Terima kasih untuk segala kerja keras sehingga penulis dapat menempuh pendidikan sejauh ini.
2. Keluarga penulis, Edwin Christian dan William Christian, yang selalu memberi semangat kepada penulis.
3. Bapak Ir. Achmad Holil Noor Ali, M.Kom., dan Ibu Anisah Herdiyanti, S.Kom., M.Sc., selaku dosen pembimbing yang telah meluangkan waktu untuk membimbing dan memberikan motivasi untuk penulis dalam penyelesaian Tugas Akhir.
4. Ibu Feby Artwodini Muqtadiroh, S.Kom, M.T., dan Ibu Amna Shifia Nisafani, S.Kom, M.Sc. yang telah bersedia menjadi dosen penguji dan memberikan masukan dan wawasan lebih untuk penulis.

5. Ketua Jurusan Sistem Informasi ITS, Bapak Dr. Eng. Fabriliyan Samopa, S.Kom., M.Kom.
6. Bapak Dr. Apol Pribadi Subriadi, S.T., M.T., selaku dosen wali penulis yang senantiasa memberikan pengarahan dan motivasi selama penulis menempuh masa perkuliahan dan pengerjaan Tugas Akhir.
7. Mbak Indri Sulistiyowati, selaku Kepala Seksi Keamanan Data Direktorat Sistem Informasi Universitas Airlangga atas bimbingan, pengarahan dan motivasinya selama pengerjaan Tugas Akhir.
8. Bapak Hermono, selaku laboran serta Aula Ayubi, faiz Fanani, dan Muhammad Nashief, selaku admin Laboratorium Perencanaan dan pengembangan Sistem Informasi (PPSI) yang turut membantu penulis menyelesaikan Tugas Akhir ini dengan baik.
9. Teman-teman mahasiswa Sistem Informasi BASILISK dan Laboratorium PPSI yang telah memberikan semangat dan meluangkan waktu untuk berdiskusi dengan penulis.
10. Teman-teman pemuda GSJA Maranatha Malang atas doa dan dukungan yang diberikan.
11. Pihak-pihak lain yang tidak dapat penulis sebutkan satu persatu, yang telah membantu penulis dalam pengerjaan Tugas Akhir ini.

Penulis menyadari bahwa masih banyak terdapat kekurangan dari laporan Tugas Akhir ini, baik dari materi maupun cara penyajiannya. Maka dari itu, penulis sangat menerima kritik dan saran yang membangun untuk perbaikan di masa depan. Akhirnya, penulis berharap Tugas Akhir ini dapat bermanfaat bagi objek studi dan bagi semua pihak.

Surabaya, Juni 2015

Penulis

DAFTAR ISI

ABSTRAK v
ABSTRACT vii
KATA PENGANTAR ix
DAFTAR ISI xi
DAFTAR TABEL xv
DAFTAR GAMBAR xvii
BAB I PENDAHULUAN 1
1.1. Latar Belakang 1
1.2. Perumusan Masalah 3
1.3. Batasan Masalah 3
1.4. Tujuan Tugas Akhir 4
1.5. Manfaat Tugas Akhir 4
1.6. Relevansi Tugas Akhir 4
BAB II TINJAUAN PUSTAKA 7
2.1. Penelitian Sebelumnya 7
2.2. Audit 9
2.2.1. Pengertian Audit 9
2.2.2. Audit Teknologi Informasi 10
2.2.3. Audit Keamanan Informasi 11
2.2.4. Proses Audit 13
2.2.5. Audit Teknologi Informasi berbasis Risiko 17
2.2.6. Panduan Audit 18
2.3. Aset Informasi 21
2.4. Risiko TI 22
2.5. *Failure Mode Effect Analysis* (FMEA) 23
2.6. *Information Secutity Management System* (ISMS) 31
2.7. ISO 27002 Klausul Keamanan Fisik dan Lingkungan 32

BAB III METODOLOGI PENELITIAN 37
3.1 Tahapan Pelaksanaan Penelitian.....37
3.1.1. Tahap Perancangan.....37
3.1.2. Tahap Implementasi 38
3.1.3. Tahap Pembahasan Hasil.....41

BAB IV PERANCANGAN 45
4.1 Perancangan Studi Kasus.....45
4.1.1 Tujuan Studi Kasus.....45
4.1.2 Unit of Analysis.....46
4.2 Persiapan Pengumpulan Data 48
4.3 Metode Pengolahan Data.....49
4.4 Pendekatan Analisis.....49

BAB V IMPLEMENTASI 51
5.1. Analisis Kondisi Kekinian Organisasi.....51
5.1.1. Gambaran Umum Direktorat Sistem Informasi Universitas Airlangga.....51
5.1.2. Struktur Organisasi Direktorat Sistem Informasi 53
5.2. Penentuan Objek Penelitian.....55
5.3. Penyusunan Dokumen *Audit Plan* DSI Universitas Airlangga 55
5.3.1. Tujuan Dokumen *Audit Plan* 55
5.3.2. Penyusunan Bagian Informasi Umum.....55
5.3.3. Penyusunan Bagian Proses Audit 56
5.3.4. Penyusunan Bagian Evaluasi.....57
5.4. Verifikasi Dokumen *Audit Plan* 57
5.5. Identifikasi Aset Ruang Server Direktorat Sistem Informasi 58
5.6. Penilaian dan Analisis Risiko TI 60
5.6.1. Pendefinisian TI untuk Risiko yang Dianalisis 60
5.6.2. Identifikasi Risiko 60
5.6.3. Penilaian Risiko.....61

5.7. Pemetaan Risiko terhadap Kontrol ISO/IEC 27002:2013 Klausul Keamanan Fisik dan Lingkungan 72
5.8. Penyusunan Dokumen *Audit Program* 81
5.8.1. Komposisi Dokumen 81
5.8.2. Pembuatan Prosedur Audit 82
5.8.3. Pembuatan Pelaksanaan Tindak lanjut 86
5.9. Penyusunan Dokumen Panduan Penggunaan Audit Program 87

BAB VI HASIL DAN PEMBAHASAN 91
6.1. Verifikasi Dokumen Prosedur Audit 91
6.2. Contoh Pengisian Dokumen Prosedur Audit 95
6.3. Persetujuan Panduan Audit 102
6.3.1. Perencanaan Proses Persetujuan 102
6.3.2. Hasil Persetujuan Panduan Audit 103

BAB VII KESIMPULAN DAN SARAN 107
7.1. Kesimpulan 107
7.2. Saran 108

DAFTAR PUSTAKA 109

LAMPIRAN A. HASIL WAWANCARA A-1

LAMPIRAN B. JADWAL AKTIVITAS AUDIT B-1

LAMPIRAN C. HASIL PENILAIAN RISIKO DENGAN METODE FMEA C-1

LAMPIRAN D. VERIFIKASI PROSEDUR AUDIT D-1

LAMPIRAN E. PERSETUJUAN DOKUMEN PANDUAN AUDIT E-1

BIODATA PENULIS 113

Halaman ini sengaja dikosongkan

DAFTAR TABEL

Tabel 2. 1 Perbandingan Penelitian Sebelumnya 7
Tabel 2. 2 Kontrol Audit Keamanan Informasi..... 12
Tabel 2. 3 Parameter Severity 25
Tabel 2. 4 Parameter Occurance 26
Tabel 2. 5 Parameter Detection 27
Tabel 2. 6 Level Prioritas Nilai RPN 29
Tabel 2. 7 Control Objective ISO 27002 Klausul Keamanan Fisik dan Lingkungan..... 32
Tabel 5. 1 Verifikasi Audit Plan dengan Organisasi 58
Tabel 5. 2 Verifikasi Daftar Aktivitas Audit..... 58
Tabel 5. 3 Daftar Aset Ruang Server Universitas Airlangga . 59
Tabel 5. 4 Risiko aset TI 61
Tabel 5. 5 *Risk Register*..... 62
Tabel 5. 6 Penilaian risiko dengan FMEA 70
Tabel 5. 7 Pemetaan Risiko terhadap ISO 27002..... 73
Tabel 5. 8 Daftar Prosedur Audit 83
Tabel 6. 1 Verifikasi Dokumen Audit Prosedur P.1.1..... 91
Tabel 6. 2 Contoh Pengisian Prosedur Audit 96
Tabel A. 1 Wawancara Pengajuan Tugas Akhir A-2
Tabel A. 2 Wawancara Kondisi Kekinian Organisasi.....A-2
Tabel A. 3 Wawancara Kegiatan Audit di DSI UA A-5
Tabel A. 4 Wawancara Penerapan ISO 27002 kalusul 11 di DSI A-7
Tabel A. 5 Wawancara Aset TI di ruang server A-8
Tabel A. 6 Wawancara Aset TI di ruang server (2) A-8
Tabel A. 7 Wawancara Aset TI di ruang server (3) A-9
Tabel A. 8 Verifikasi Penilaian Risiko.....A-10
Tabel A. 9 Verifikasi Penilaian Risiko (2).....A-11
Tabel A. 10 Verifikasi dokumen Audit Plan.....A-12
Tabel A. 11 Verifikasi Dokumen Audit Program A-13
Tabel B. 1 Hasil Penilaian Risiko Aset TI DSI UA dengan Metode FMEA B-3

Tabel C. 1 Hasil Penilaian Risiko Aset TI DSI UA dengan Metode FMEA.....C-3
Tabel D. 1 Verifikasi Dokumen Prosedur Audit P.1.1 ..... D-3
Tabel D. 2 Verifikasi Dokumen Prosedur Audit P.1.2 ..... D-6
Tabel D. 3 Verifikasi Dokumen Prosedur Audit P.1.3 ..... D-8
Tabel D. 4 Verifikasi Dokumen Prosedur Audit P.1.4 ..... D-10
Tabel D. 5 Verifikasi Dokumen Prosedur Audit P.1.5 ..... D-10
Tabel D. 6 Verifikasi Dokumen Prosedur Audit P.1.6 ..... D-12
Tabel D. 7 Verifikasi Dokumen Prosedur Audit P.2.1 ..... D-14
Tabel D. 8 Verifikasi Dokumen Prosedur Audit P.2.2 ..... D-17
Tabel D. 9 Verifikasi Dokumen Prosedur Audit P.2.3 ..... D-18
Tabel D. 10 Verifikasi Dokumen Prosedur Audit P.2.4 .... D-19
Tabel D. 11 Verifikasi Dokumen Prosedur Audit P.2.5 .... D-21
Tabel D. 12 Verifikasi Dokumen Prosedur Audit P.2.6 .... D-23
Tabel D. 13 Verifikasi Dokumen Prosedur Audit P.2.7 .... D-25
Tabel D. 14 Verifikasi Dokumen Prosedur Audit P.2.8 .... D-26
Tabel D. 15 Verifikasi Dokumen Prosedur Audit P.2.9 .... D-27

DAFTAR GAMBAR

Gambar 1. 1 Research Roadmap Lab PPSI 5
Gambar 2. 1 Proses Audit [13] 17
Gambar 2. 2 Intisari Proses Audit Berbasis Risiko 18
Gambar 2. 3 Tahapan FMEA [19] 24
Gambar 2. 4 Contoh Penilaian dengan Metode FMEA 30
Gambar 3. 1 Metodologi Peneliti 43
Gambar 4. 1 Hubungan Unit of Analysis dengan Tipe Studi Kasus 47
Gambar 5. 1 Struktur Organisasi Direktorat Sistem Informasi 53
Gambar 5. 2 Diagram Kerja Direktorat Sistem Informasi 54
Gambar 5. 3 Contoh Prosedur Audit 84
Gambar 5. 4 Contoh Hirarki Prosedur Audit 85
Gambar 5. 5 Contoh Kesimpulan Temuan Audit 86
Gambar 5. 6 Formulir Pelaksaan Tindak Lanjut Audit 87
Gambar 5. 7 Contoh Isi Panduan Penggunaan Audit Program 89

Halaman ini sengaja dikosongkan

BAB I
PENDAHULUAN

Pada bab pendahuluan akan diuraikan proses indentifikasi masalah penelitian yang meliputi latar belakang masalah, perumusan masalah, batasan masalah, tujuan tugas akhir, dan manfaat kegiatan tugas akhir. Berdasarkan uraian pada bab ini, harapannya gambaran umum permasalahan dan pemecahan masalah pada tugas akhir dapat dipahami.

1.1. Latar Belakang

Perkembangan Teknologi Informasi (TI) yang sangat pesat dewasa ini telah menjadi bagian penting dari organisasi. Keuntungan yang dapat dirasakan dengan jelas adalah penurunan biaya usaha dengan tingkat pelayanan membaik, kepuasan meningkat dan omset meningkat tinggi. Penerapan TI sangat mendukung kinerja suatu organisasi, dimana inovasi TI sebagai faktor penting [1]. Oleh karena itu TI mulai dikembangkan untuk pendidikan Perguruan Tinggi untuk mendukung kegiatan operasional seperti administrasi, belajar mengajar, melakukan riset, mengembangkan TI dengan menghasilkan *software* dan *hardware*, dan menghasilkan Sumber Daya Manusia (SDM) yang menguasai TI [2].

Implementasi teknologi informasi memerlukan sistem keamanan yang memadai. Salah satu keamanan yang harus diperhatikan adalah keamanan fisik dan lingkungan TI. Keamanan Fisik dan Lingkungan TI di sini meliputi tata letak, kondisi infrastruktur, fasilitas TI yang tersedia, pengamanan akses fisik itu sendiri, penempatan kabel, pemindahan dan pembuangan komponen TI yang sensitif, serta perawatan

peralatan TI. Keamanan fisik dan lingkungan TI ini mencegah kehilangan dan/atau kerusakan data yang diakibatkan oleh lingkungan secara fisik, termasuk bencana alam dan pencurian data yang tersimpan dalam media penyimpanan atau dalam fasilitas penyimpan informasi yang lain [3].

Direktorat Sistem Informasi (DSI) sebagai pusat pengembangan teknologi informasi Universitas yang membawahi dua Sub Dit, yakni Sub Dit Pengolahan Data dan Sub Dit Pengembangan Sistem. Visi DSI adalah "*menunjang terealisasinya visi institusional Unair untuk menjadi Perguruan Tinggi yang mandiri, inovatif, terkemuka, pelopor pengembangan ilmu pengetahuan, teknologi, humaniora, dan seni, berdasarkan moral agama, melalui ketersediaan sistem dan teknologi informasi yang handal dan terpercaya.*" Direktorat Sistem Informasi Universitas Airlangga telah mengadopsi standar ISO/IEC 27001 dan 27002 sebagai standar manajemen keamanan informasi. Audit TI/SI juga telah beberapa kali dilakukan oleh pihak Direktorat Sistem Informasi Universitas Airlangga, namun pelaksanaan audit ini belum memiliki bakuan. Bakuan atau panduan audit merupakan kumpulan kertas yang dijilid yang berisi tulisan sebagai panduan untuk melakukan proses audit bagi auditor, yang terdiri dari *audit charter, audit plan*, dan *audit program*. Tidak adanya bakuan/panduan audit ini dapat menyebabkan tidak terstrukturnya proses audit yang dilakukan, seperti auditor tidak mengetahui informasi penting yang diperlukan saat audit. Sehubungan dengan belum adanya panduan audit TI dan pentingnya kemananan fisik dan lingkungan TI serta adanya visi DSI yang menyatakan bahwa dibutuhkannya teknologi informasi yang handal dan terpercaya untuk mencapi tujuan yang ada, maka diperlukan panduan audit TI di Direktorat Sistem Informasi di bagian Keamanan Fisik dan Lingkungan TI.

Penelitian tugas akhir ini bertujuan untuk menghasilkan panduan audit teknologi informasi untuk pengelolaan keamanan fisik dan lingkungan TI pada Direktorat Sistem Informasi Universitas Airlangga berdasarkan ISO/IEC 27002 yang digunakan. Hasil dari tugas akhir ini akan terdiri atas penjelasan mengenai tujuan, ruang lingkup, informasi auditee dan auditor, acuan dan penanggung jawab audit, prosedur audit, audit checklist, dan formulir lain yang mendukung proses audit TI. Pembuatan panduan audit ini diharapkan dapat membantu auditor untuk melakukan proses audit di bagian ini lebih terstruktur.

1.2. Perumusan Masalah

Berdasarkan uraian latar belakang di atas, maka rumusan permasalahan yang menjadi fokus dan akan diselesaikan dalam Tugas Akhir yaitu **bagaimana hasil panduan audit pengelolaan Keamanan Fisik dan Lingkungan TI di Direktorat Sistem Informasi Universitas Airlangga** dengan sub rumusan masalah sebagai berikut:

1. Bagaimana usulan *audit plan* yang dibuat?
2. Apa sajakah risiko teknologi informasi yang terdapat pada Direktorat Sistem Informasi Airlangga terkait dengan pengelolaan keamanan fisik dan lingkungan?
3. Apa sajakah *control objective* dan panduan implementasi yang dapat memitigasi risiko yang ada?
4. Bagaimana usulan *audit program* yang dibuat?

1.3. Batasan Masalah

Dalam pengerjaan tugas akhir ini, ada beberapa batasan masalah yang harus diperhatikan, yaitu sebagai berikut:

1. Dokumen panduan audit SI/TI difokuskan pada 2 (dua) bagian yaitu Dokumen *Audit Plan* dan *Audit Program*.
2. Dokumen panduan audit SI/TI yang dihasilkan akan difokuskan pada aspek pengelolaan Keamanan Fisik dan Lingkungan TI di salah satu ruang kerja Direktorat Sistem Informasi Universitas Airlangga.

1.4. Tujuan Tugas Akhir

Tujuan pembuatan tugas akhir ini adalah untuk menghasilkan dokumen panduan audit pengelolaan Keamanan Fisik dan Lingkungan TI yang dapat digunakan untuk acuan pelaksanaan audit pada Direktorat Sistem Informasi Universitas Airlangga berdasarkan ISO/IEC 27002:2013 serta pemberian contoh dalam penggunaannya.

1.5. Manfaat Tugas Akhir

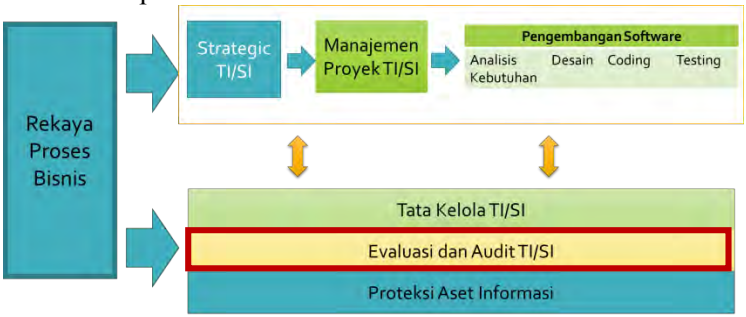
Manfaat yang dapat diperoleh dari pengerjaan tugas akhir ini adalah:

1. Mengetahui risiko mengenai Keamanan Fisik dan Lingkungan TI di area Direktorat Sistem Informasi Universitas Airlangga agar dampak risiko tersebut dapat diminimalisir.
2. Membantu auditor internal organisasi dalam pelaksanaan audit SI/TI lebih terstruktur.

1.6. Relevansi Tugas Akhir

Tugas akhir ini berkaitan dengan mata kuliah Audit SI/TI dalam kaitannya proses menyusun dokumen panduan audit dan Manajemen Risiko Teknologi Informasi (MRTI) dalam

kaitannya penilaian risiko dalam menentukan ruang lingkup audit yang akan dilakukan. Dalam roadmap penelitian Laboratorium PPSI masalah tersebut terletak pada Evaluasi dan Audit SI/TI. Peta jalan penelitian (research roadmap) tersebut bisa dilihat pada Gambar 1.1 dibawah ini.



Gambar 1. 1 Research Roadmap Lab PPSI

Halaman ini sengaja dikosongkan

BAB II
TINJAUAN PUSTAKA

Bab ini akan menjelaskan mengenai penelitian sebelumnya dan dasar teori yang dijadikan acuan atau landasan dalam pengerjaan tugas akhir ini. Landasan teori akan memberikan gambaran secara umum dari landasan penjabaran tugas akhir ini.

2.1. Penelitian Sebelumnya

Terdapat sedikit literatur yang menjelaskan mengenai pembuatan perangkat audit dan panduan audit. Tabel 2.1 menyajikan penelitian-penelitian sebelumnya yang sedikit menyinggung mengenai pembuatan panduan audit teknologi informasi.

Tabel 2. 1 Perbandingan Penelitian Sebelumnya

	Penelitian 1	Penelitian 2	Penelitian 3
Nama Peneliti	Mochammad Arief Ramadhan (2011)	Pandu Gilas Anarkhi (2012)	Yudhis Cahyo Eko (2013)
Judul Penelitian	Pembuatan Perangkat Audit Internal TI berbasis Resiko menggunakan ISO/IEC 27002:2007 pada Proses Pengelolaan Data Studi Kasus Digital Library ITS [4]	Penyusunan Perangkat Audit Kemanan Informasi Aplikasi Berbasis Web menggunakan ISO/IEC 27001 Klausul Kendali Akses [5]	Pembuatan Panduan Audit Teknologi Informasi pada Proses Pengelolaan Lingkungan Fisik berbasis COBIT 5 di KPPN Surabaya II [6]

	Penelitian 1	Penelitian 2	Penelitian 3
Hasil Penelitian	Penelitian ini berisi pembuatan perangkat audit yang berupa *audit checklist* pada Digital Library ITS yang mengacu pada pemetaan ISO/IEC 27002:2007. Di dalam ISO 27002:2007 ini juga telah terdapat standar pengelolaan keamanan.	Penelitian ini berisi pembuatan perangkat audit berupa *checklist audit* dengan acuan ISO/IEC 27001 klausul kendali akses pada aplikasi web milik Universitas Airlangga. Hal-hal yang akan diaudit antara lain Direktur Sistem Informasi, administrator, database, dan peraturan lain yang terkait.	Penelitian ini berisi pembuatan panduan audit yang berbasis pada COBIT 5. Panduan Audit yang dibuat meliputi ikhtisar dokumen panduan audit, kertas kerja pemeriksaan utama, *audit checklist*, prosedur audit, dan kertas kerja konsep temuan.
Kelebihan	Menggunakan ISO/IEC 27002:2007 dalam pemetaan risiko sehingga pembuatan perangkat audit, khususnya *audit checklist* lebih mudah dan terstruktur.	Organisasi telah menerapkan ISO/IEC 27001 dalam proses bisnis terutama dalam bidang keamanan sehingga penggunaan standar ini akan menghasilkan keluaran yang pas.	Pembuatan produk audit dari penelitian ini lebih rinci dan dapat menuntun auditor langkah demi langkah. COBIT 5 juga membuat penilaian proses lebih efektif.
Kekurangan	Produk perangkat audit yang dihasilkan hanya sebatas *audit checklist* saja, tanpa rekomendasi atau review dari auditornya, sehingga hasil yang didapatkan nantinya hanya terbatas pada sesuai atau tidak sesuai saja.	Tidak adanya contoh verifikasi untuk perangkat audit yang telah dibuat, sehingga tidak diketahui apakah dokumen perangkat yang dibuat telah sesuai dengan kebutuhan instansi atau belum.	*Breakdown* struktur dokumen panduan audit masih membingungkan. Verifikasi dokumen pun dilaukan hanya sebatas pengecekan kelengkapan dokumen saja tanpa verifikasi dengan pihak KPPN II

	Penelitian 1	Penelitian 2	Penelitian 3
Relevansi Penelitian	Penulis menggunakan penelitian ini untuk membantu dalam mengerjakan Tugas Akhir dalam hal pemetaan dalam ISO/IEC 27002. Dengan menggunakan standar yang sama diharapkan pemetaan yang dilakukan penulis lebih tepat.	Organisasi tempat penelitian dilakukan, menguatkan penulis untuk melakukan Tugas Akhir dengan topik audit namun ruang lingkup yang berbeda dengan penelitian 2 ini.	Fokus penelitian saat ini adalah membuat panduan audit, sama dengan apa yang dilakukan pada penelitian 3 ini sehingga akan memudahkan penulis untuk mengetahui apa saja yang harus disusun dalam panduan audit.

2.2. Audit

Pada bagian ini akan dijelaskan mengenai pengertian Audit, Audit TI, Audit Keamanan Informasi, Audit Berbasis Risiko, dan proses audit.

2.2.1. Pengertian Audit

Alvin A. Arens dan James K. Loebbecke [7] mendefinisikan audit yaitu:

"Auditing adalah salah satu set prosedur yang sesuai dengan norma pemerikasaan akuntan yang memberikan informasi sehingga akuntan dapat menyatakan suatu pendapat tentang laporan keuangan yang diperiksa disajikan secara wajar sesuai dengan Prinsip Kuntansi yang berlaku".

Pengertian auditing adalah suatu pemeriksaan yang dilakukan secara kritis dan sistematis, oleh pihak yang independen, terhadap laporan keuangan yang telah disusun oleh pihak manajemen beserta catatan-catatan pembukuan dan bukti-bukti

pendukungnya, dengan tujuan untuk daat memberikan pendapat mengenai laporan kewajaran laporan keuangan tersebut. [8]

Sedangkan pengrtian audit menurut PSAK – Tim Sukses UKT Akuntansi 2006 adalah suatu proses sistematik yang bertujuan untuk memperoleh dan mengevaluasi bukti yang dikumpulkan atas pernyataan atau asersi tentang aksi-aksi dan kejadian-kejadian dan melihat bagaimana tingkat hubungan antara pernyataan atau asersi dengan kenyataan dan mengkomunikasikan hasilnya kepada yang berkepentingan.

Sehingga dapat dikatakan bahwa audit adalah pemeriksaan terhadap proses yang telah dilakukan pada masa lampau dengan cara mengumpulkan bukti-bukti yang terkait, dengan tujuan untuk mendapatkan laporan kesesuaian antara proses yang dilakukan dengan standar yang diacu.

2.2.2. Audit Teknologi Informasi

Audit TI atau audit SI (Sistem Informasi) adalah bentuk pemeriksaan dan pengendalian dari infrastruktur TI secara menyeluruh. Pada mulanya istilah ini dikenal dengan audit pemrosesan data elektronik, dan sekarang audit TI secara umum merupakan proses pengumpulan dan evaluasi dari semua kegiatan sistem informasi dalam perusahaan itu. Dalam salah satu buku Information System Controls and Audit [9] menyatakan beberapa alasan penting mengapa audit TI perlu dilakukan, antara lain:

1. Kerugian akibat kehilangan data.
   Akibat terjadinya gangguan virus atau terjadi kebakaran pada ruangan komputer yang dimiliki akan mengakibatkan seluruh data hilang. Kehilangan data akan mengakibatkan perusahaan tidak dapat melakukan pengecekan data.

2. Kesalahan dalam pengambilan keputusan.
   Banyak kalangan usaha yang saat ini telah menggunakan bantuan Decision Support System (DSS) untuk mengambil keputusan-keputusan penting. Risiko yang muncul apabila terjadi kesalahan memasukkan data ke sistem TI yang digunakan.
3. Risiko kebocoran data.
   Data bagi sebagian besar sektor usaha merupakan sumber daya yang tidak ternilai harganya. Kebocoran data ini akan berdampak terhadap kehilangan sejumlah sejumlah data dan dapat mengganggu kelangsungan hidup perusahaan.
4. Tingginya nilai investasi perangkat keras dan perangkat lunak komputer.
   Investasi yang dikeluarkan untuk suatu proyek TI seringkali sangat besar. Bahkan, dari penelitian yang pernah dilakukan [10],tercatat bahwa 20% pengeluaran TI terbuang secara percuma, 30-40% proyek TI tidak mendatangkan keuntungan. Selain itu, sulit mengukur manfaat yang dapat diberikan TI.

2.2.3. Audit Keamanan Informasi

Audit keamanan informasi merupakan audit yang mencakup audit akses fisik dan audit akses logis. Kontrol yang diaudit dapat dikategorikan ke teknis, fisik dan administrasi. [11] Beberapa jenis kontrol yang diaudit dalam audit keamanan informasi disajikan dalan tabel 2.2

Tabel 2. 2 Kontrol Audit Keamanan Informasi

	Preventive	***Detective***
Physical	• *locks and keys* • *backup power* • *biometric access controls* • *site selection* • *fire extinguishers*	• *motion detectors* • *smoke and fire detectors* • *CCTV monitors* • *sensors and alarms*
Technical	• *authentication* • *Firewalls & IPS* • *anti-virus software* • *encryption* • *access control* • *Vulnerabilities assessment* • *Diagnostic reviews*	• *audit trails* • *intrusion detection* • *automated configuration monitoring* • *penetration testing*
Administrative	• *employment procedures* • *supervision* • *technical training* • *separation of duties* • *disaster recovery plans* • *security awareness training* • *Diagnostic reviews…*	• *security reviews and audits* • *performance evaluations* • *required vacations/rotation of duties* • *incident investigations*

Ketika audit berpusat pada aspek keamanan informasi TI, audit tersebut dapat dilihat sebagai bagian dari audit teknologi informasi. Hal ini kemudian sering disebut sebagai audit keamanan teknologi informasi atau audit keamanan komputer [12]. Namun, audit keamanan informasi ruang lingkupnya lebih dari aset TI yang ada.

2.2.4. Proses Audit

Proses Audit menurut ISO 19011 [13] terdiri atas:

1. *Initiating the Audit*
Ketika sebuah audit dimulai, tanggung jawab atas terselenggaranya audit ada pada ketua tim audit yang ditugaskan hingga audit tersebut telah selesai (Gambar 2.2 bagian 6.6). Langkah-langkah audit seperti pada gambar 2.2 perlu diperhatikan, namun langkah-langkah tersebut dapat berbeda tergantung pada *auditee* dan ruang lingkup serta keadaan audit.

Dalam tahap awal memulai audit terdapat 2 hal yang perlu diperhatikan, yaitu

1.1 Pertemuan awal dengan auditee

Pertemuan awal ini dapat diadakan secara formal atau informal. Tujuan dari pertemuan ini adalah untuk membicarakan segala hal mengenai audit yang akan dilakukan - termasuk jadwal, tim audit, ruang lingkup audit, *auditee* – dan penyerahan tanggung jawab kepada ketua tim auditor.

1.2 Menentukan kemungkinan audit

Kemungkinan audit harus ditentukan untuk dapat memastikan tujuan dari audit dapat dicapai dengan baik. Ketika audit yang akan dilaksanakan terlihat tidak memungkinkan, auditor harus mengajukan perubahan pada *client*, tentunya dengan persetujuan *auditee*.

2. *Preparing audit activities*
Hal yang perlu diperhatikan dalam tahap persiapan aktivitas audit adalah

2.1 Meninjau dokumen sistem manajemen untuk persiapan audit

Proses ini dilakukan agar auditor dapat mengumpulkan informasi untuk dapat digunakan pada audit selanjutnya. Dokumen yang harus di-*review* antara lain dokumen sistem manajemen dan catatan-catatannya serta laporan audit sebelumnya.

2.2 Menyiapkan dokumen *audit plan*

Ketua tim audit harus menyiapkan *audit plan* berdasarkan informasi yang ada pada audit program dan pada dokumen yang telah disediakan oleh *auditee*. Detil yang ada pada *audit plan* harus berdasarkan pada ruang lingkup dan kompleksitas audit yang dilaksanakan. *Audit plan* harus sedapat mungkin fleksibel terhadap perubahan yang mungkin diperlukan saat aktivitas audit berlangsung.

Audit plan harus mencakup atau merujuk hal-hal berikut ini:

a. Tujuan audit
b. Ruang lingkup audit
c. Kriteria audit
d. Lokasi, tanggal, waktu yang direncanakan dan durasi audit dilaksanakan, termasuk rapat dengan pihak manajemen *auditee*
e. Metode audit yang akan digunakan
f. Peran dan tanggung jawab anggota tim audit

Audit plan harus dipresentasikan pada *auditee*. Kerancuan terhadap apa yang ada di *audit plan* haruslah diselesaikan antara *auditee*, *audit client,* dan auditor.

2.3 Pemberian tugas pada tim audit

Ketua tim audit berhak memberikan tanggung jawab kepada setiap anggota tim audit untuk mengaudit proses,

aktivitas fungsi, atau lokasi tertentu. Perubahan terhadap tugas yang diberikan dapat dilakukan saat proses audit berlangsung untuk memastikan tujuan audit terpenuhi.

2.4 Menyiapkan dokumen kerja

Anggota tim audit harus mengumpulkan dan meninjau ulang informasi yang berkaitan dengan tugas audit masing-masing anggota dan menyiapkan dokumen kerja. Dokumen kerja yang dimaksud antara lain adalah:
a. *checklist*
b. rencana *audit sampling*
c. formulir untuk pencatatan bukti audit, temuan audit, dan catatan rapat.

3. *Conducting the audit activities*

Aktivitas audit umumnya dilaksanakan seperti yang tertera pada Gambar 2.2 yaitu:

a. Melakukan *kick-off meeting*
b. Melakukan *review* dokumen saat audit berlangsung
c. Berkomunikasi dengan tim saat audit
d. Pemberian tugas dan tanggung jawab pada pemantau audit
e. Mengumpulkan dan memverifikasi informasi
f. Membuat temuan audit
g. Menyiapkan simpulan audit
h. Melakukan *closing meeting*

4. *Preparing and distributing the audit report*

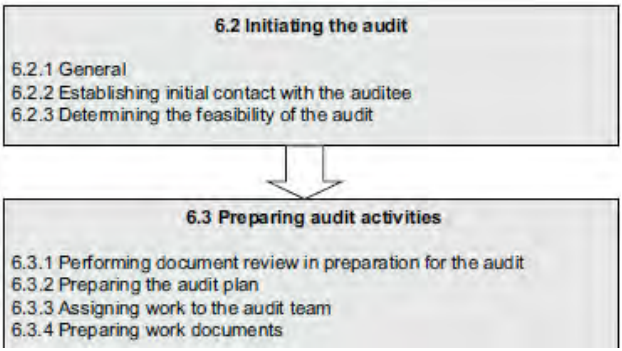
Ketua tim audit harus melaporkan hasil audit yang dilakanakan berdasarkan audit program. Laporan audit juga harus dikeluarkan dalam kurun waktu yang disetujui. Jika waktu tidak sesuai, auditor harus mengomunikasikan alasan keterlambatan kepada *auditee*. Selain itu laporan audit juga harus di beri tanggal dan disetujui oleh pihak *auditee*.

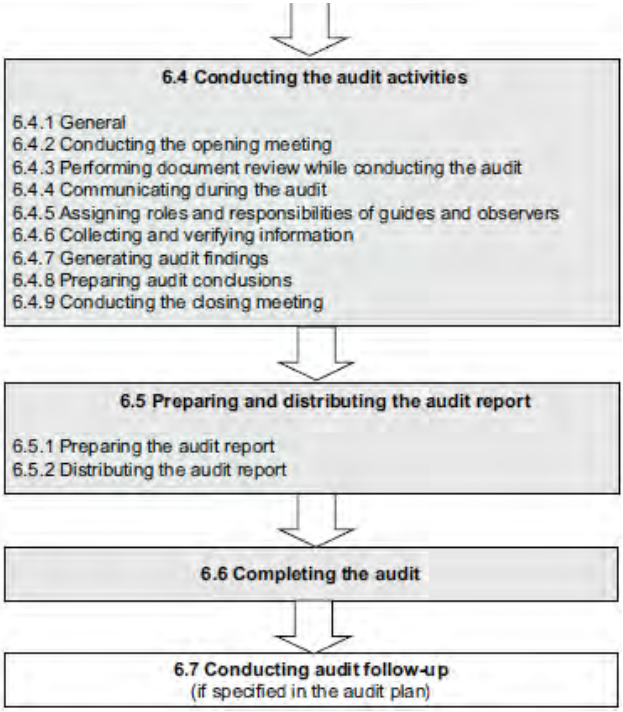
5. *Completing the audit*
Audit telah selesai ketika semua rencana aktivitas audit telah dilaksanakan dan diselesaikan, atau telah disetujui oleh *audit client* (hal in dapat terjadi ketika audit tidak dapat berjalan sesuai rencana).

Dokumen yang verkaitan dengan audit dapat disimpan atau dihancurkan sesuai dengan persetujuan pihak yang terlibat dalam audit program. Pembelajaran yang didapat saat audit harus dicatat dalam sistem manajemen organisasi yang diaudit.

6. *Conducting audit follow-up*
Kesimpulan dari audit yang dilakukan mungkin saja memerlukan perbaikan, baik itu aksi *corrective, preventive,* atau *improvement*. Kegiatan tersebut biasanya dilakukan oleh *auditee* dalam kurun waktu tertentu yang sudah disetujui. *Auditee* juga harus menghubungi dan mnegkomunikasikan ti audit mengenai status kegiatan perbaikan yang dilakukan.

Dari seluruh proses yang ada (proses 1-6) dalam pengerjaan Tugas Akhir ini hanya akan digunakan proses 1 dan 2 yaitu *initiating the* audit dan *preparing audit* activities dimana fokus dari dua proses ini adalah planning dari kegiatan audit. Tahap 3 sampai 6 tidak akan dilakukan oleh penulis karena penulis tidak sampai pada tahap melakukan proses audit.



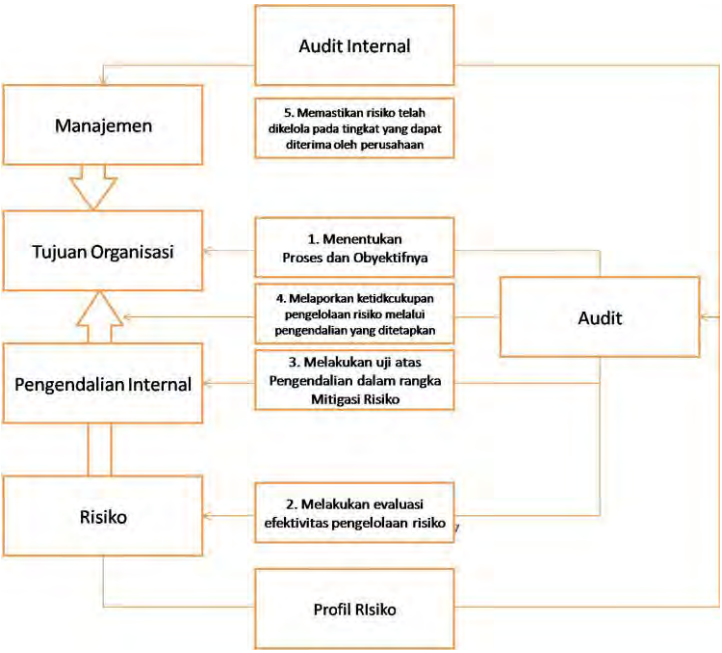


Gambar 2. 1 Proses Audit [13]

2.2.5. Audit Teknologi Informasi berbasis Risiko

Audit Berbasis Risiko adalah metodologi pemeriksaan yang dipergunakan untuk memberikan jaminan bahwa risiko telah dikelola di dalam batasan risiko yang telah ditetapkan manajemen pada tingkatan korporasi. Ada 2 hal utama yang harus dipahami oleh internal auditor yakni aspek pengendalian dari setiap proses bisnis yang terkait, dan risiko serta faktor-faktor pengendalian guna mendukung pencapaian sasaran perusahaan. [14]

Gambar 2.2 menunjukkan intisari dari proses audit berbasis risiko.



Gambar 2. 2 Intisari Proses Audit Berbasis Risiko

2.2.6. Panduan Audit

Menurut Satriadi [15] pengertian dari Buku Panduan adalah:

"Kumpulan kertas atau bahan lainnya yang dijilid menjadi satu pada salah satu ujungnya dan berisi tulisan atau gambar yang berfungsi sebagai panduan bagi penggunanya dan setiap babnya berurutan sesuai dengan kebutuhan penggunanya.".

Buku panduan audit adalah kumpulan kertas yang dijilid yang berisi tulisan sebagai panduan untuk melakukan proses audit

bagi auditor. Tujuan dari buku audit adalah membuat para auditor dan/atau auditee mengerti proses dan informasi selama audit dilaksanakan serta membuat proses audit lebih terstruktur.

Panduan Audit secara garis besar dibagi menjadi beberapa bagian yaitu:

a. Dokumen *Audit Charter*

   Audit Charter adalah sebuah dokumen resmi yang mendefinisikan tujuan, wewenang, dan tanggung jawab aktivitas audit internal [16]. Posisi proses audit internal dalam organisasi ditetapkan dalam *Audit Charter*. Hal ini termasuk sifat hubungan pelaporan fungsional kepala Audit eksekutif dengan dewan; kewenangan akses terhadap catatan, personel, dan sifat fisik yang relevan dengan kinerja keterlibatan; dan mendefinisikan ruang lingkup kegiatan audit internal. Persetujuan akhir dari *Audit Charter* adalah dengan jajaran eksekutif.

b. Dokumen *Audit Plan*

   Audit Plan adalah pedoman khusus yang harus diikuti ketika melakukan audit. *Audit Plan* menggambarkan proses-proses yang harus dilakukan oleh auditor untuk dapat mencapai tujuan audit. Dokumen ini akan membantu auditor memperoleh bukti yang cukup dan tepat, membantu menjaga biaya audit pada tingkat yang wajar, dan membantu menghindari kesalahpahaman dengan klien.

   Menurut ISO 19011 [13] *Audit Plan* setidaknya mencakup hal-hal berikut:

   Audit plan harus mencakup atau merujuk hal-hal berikut ini:

   a. Tujuan audit
   b. Ruang lingkup audit
   c. Kriteria audit

d. Lokasi, tanggal, waktu yang direncanakan dan durasi audit dilaksanakan, termasuk rapat dengan pihak manajemen *auditee*
e. Metode audit yang akan digunakan
f. Peran dan tanggung jawab anggota tim audit

c. Dokumen *Audit Program*

Program audit dapat mencakup audit yang menilai satu atau lebih standar sistem manajemen, yang dilakukan baik secara terpisah atau dalam kombinasi.

Top Management harus memastikan bahwa tujuan program audit ditetapkan dan menetapkan satu atau lebih kompeten orang untuk mengelola program audit.Ruang lingkup program audit harus didasarkan pada ukuran dan sifat organisasi yang diaudit, serta pada sifat, fungsi, kompleksitas dan tingkat kematangan sistem manajemen yang diaudit. [13]

Menurut ISO 19011 [13], program audit harus mencakup informasi dan sumber daya yang diperlukan untuk mengatur dan melakukan audit secara efektif dan efisien dalam kerangka waktu tertentu dan juga dapat mencakup sebagai berikut:

1. Tujuan untuk program audit dan audit individu;
2. Prosedur program audit;
3. Kriteria audit;
4. Metode audit;
5. Pemilihan tim audit;
6. Sumber daya yang diperlukan, termasuk perjalanan dan akomodasi;
7. Proses untuk menangani kerahasiaan, keamanan informasi, kesehatan dan keselamatan, dan hal-hal lain yang sejenis.

Dalam pengerjaan Tugas Akhir ini, dokumen panduan audit hanya berfokus pada *Audit Plan* dan *Audit Program* saja. *Audit program* yang dibuat akan mengacu pada penelitian milik Yudhis Eko Cahyo [6], dimana akan terjadi beberapa penyesuaian. *Audit program* yang disusun penulis berisi:

a. Tujuan dan ruang lingkup audit,
b. *Best practice* dan kendali tujuan,
c. Prosedur program audit, dan
d. Dokumen kerja audit.

2.3. Aset Informasi

Aset informasi didefinisikan sebagai bagian dari informasi yang diatur dan dikelola sebagai satu kesatuan sehingga dapat dapat dipahami, dibagi, dilindungi dan dieksploitasi secara efektif. Aset Informasi merupakan hal yang paling berharga bagi organisasi karena berkaitan langsung dengan banyaknya orang yang mengakses informasi. Berikut merupakan sifat dari asset informasi:

a. Aset Informasi menjadi nilai bagi organisasi.
b. Tidak mudah diganti tanpa ada biaya, keahlian, waktu, dan sumberdaya.
c. Sebagai identitas perusahaan namun juga dapat mengancam perusahaan.

Klasifikasi kemanan asset informasi terbagi atas tiga hal yaitu [3]:

a. *Confidential*
   Informasi yang sangat berharga bagi perusahaan. Jika informasi ini bocor diluar organisasi maka akan menimbulkan kerugian atau kehilangan image perusahaan.

b.

c. *Internal Use Only*

Informasi yang hanya dapat diketahui oleh internal perusahaan. Contohnya informasi mengenai kebijakan, materi pelatihan, dll.

d. *Public*
Informasi dapat diakses oleh semua orang baik internal maupun eksternal perusahaan. Informasi yang akan di publis akan disetujui oleh pihak perusahaan.

2.4. Risiko TI

Risiko TI adalah bagian dari risiko bisnis khususnya, risiko bisnis yang terkait dengan penggunaan, kepemilikan, operasi, keterlibatan, pengaruh, dan penerapan TI dalam suatu perusahaan. Risiko TI dapat terjadi dengan frekuensi dan besaran yang tidak pasti, serta dapat berpotensi mempengaruhi bisnis dan menciptakan tantangan dalam memenuhi sasaran strategis [17].

ISACA menerbitkan *IT Risk Framework* sebagai pandangan yang komprehensif dari semua risiko yang terkait dengan penggunaan TI. Menurut ISACA, risiko TI memiliki makna yang lebih luas, yaitu bukan hanya mencakup dampak negatif dari operasi dan pelayanan yang dapat membawa kehancuran atau pengurangan nilai organisasi, tetapi juga nilai yang terkait dengan peluang yang hilang untuk menggunakan teknologi atau manajemen proyek TI dalam meningkatkan bisnis dengan dampak bisnis yang merugikan.

Risiko TI dapat dikategorikan menjadi tiga kategori [18], yaitu:
a. Manfaat TI

Risiko yang berkaitan dengan kehilangan kesempatan untuk meningkatkan nilai bisnis dengan menggunakan TI atau meningkatkan proses.

b. Program TI

Risiko yang berkaitan dengan pengelolaan proyek TI terkait yang dimaksudkan untuk meningkatkan bisnis.

c. Operasi TI

Risiko yang terkait dengan operasi dan pelayanan TI sehari-hari yang dapat membawa masalah dan ketidakefisienan terhadap operasi bisnis dari suatu organisasi.

Prinsip-prinsip risiko TI adalah sebagai berikut:

a. Selalu selaras dengan tujuan bisnis.
b. Menyeimbangkan biaya dan manfaat manajemen risiko TI.
c. Meningkatkan komunikasi risiko TI yang adil dan terbuka.
d. Menetapkan pola yang tepat sementara mendefinisikan dan menegakkan akuntabilitas.
e. Merupakan proses yang berkesinambungan dan bagian dari kegiatan sehari-hari.

Dengan melakukan analisis risiko pada penelitian ini maka diharapkan pembuatan panduan audit dapat fokus ke risiko yang penting. Nantinya analisis risiko juga dapat membantu pihak DSI Unair untuk meminimalkan dampak terhadap risiko yang ada.

2.5. *Failure Mode Effect Analysis* (FMEA)

Failure Mode and Effect Analysis atau FMEA merupakan metode yang digunakan untuk mengidentifikasi dan mencegah mode kegagalan. Tujuan dari FMEA adalah sebagai berikut:

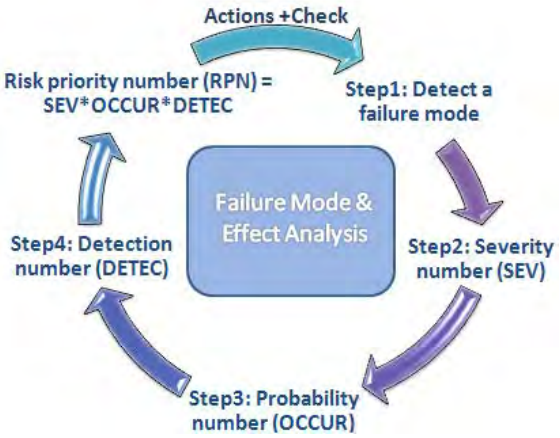
1. Mengenal dan memprediksi potensial kegagalan dari produk atau proses yang dapat terjadi.
2. Memprediksi dan mengevaluasi pengaruh dari kegagalan pada fungsi dalam sistem yang ada.

3. Menunjukkan prioritas terhadap perbaikan suatu proses atau sub sistem melalui daftar peningkatan proses atau sub sistem yang harus diperbaiki.
4. Mengidentifikasi dan membangun tindakan perbaikan yang bisa diambil untuk mencegah atau mengurangi kesempatan terjadinya potensi kegagalan atau pengaruh pada sistem.
5. Mendokumentasikan proses secara keseluruhan.

FMEA mengidentifikasikan tiga hal, yaitu [19]:

1. Penyebab kegagalan dari sistem, desain produk, serta proses selama siklus hidupnya.
2. Efek dari kegagalan.
3. Tingkat kekritisan efek dari suatu kegagalan.

Proses yang dilakukan dalam penerapan FMEA adalah mengukur potensi terjadinya kegagalan tersebut melalui tiga komponen. Tahapan dari FMEA digambarkan pada diagram alur gambar 2.3 berikut.



Gambar 2. 3 Tahapan FMEA [19]

Komponen kegagalan tersebut adalah sebagai berikut:

a) S = *Severity* (tingkat keparahan) / *Impact*

Severity atau keseriusan efek kegagalan merupakan pengukuran dalam memperkirakan subjektif numerik dari seberapa parah efek kegagalan yang akan dirasakan oleh pengguna akhir. Berikut ini adalah ukuran parameter dari *severity* [20].

Tabel 2. 3 Parameter Severity

Rank	*Effect*	*Severity of effect*
1	*None*	*No effect*
2	*Very Slight*	*Negligible effect on product performance. User not affected.*
3	*Slight*	*Slight effect on product performance. Non-vital faults will be noticed most of the time.*
4	*Minor*	*Minor effect on product performance. User slightly dissatisfied.*
5	*Moderate*	*Reduced performance with gradual performance degradation. User dissatisfied.*
6	*Severe*	*Product operable and safe but performance degraded. User dissatisfied.*
7	*High Severity*	*Product performance severely affected. User very dissatisfied.*
8	*Very High Severity*	*Product inoperable but safe. User very dissatisfied.*
9	*Extreme Severity*	*Product failure resulting in hazardous effects highly probable. Compliance with government regulations in jeopardy.*

Rank	*Effect*	*Severity of effect*
10	*Maximum Severity*	*Product failure resulting in hazardous effects almost certain. Non-compliance with government regulations.*

b) O = *Occurance* (tingkat kejadian) / *Likelihood*

Occurance atau frekuensi kegagalan merupakan pengukuran dalam memperkirakan subjektif numerik dari probabilitas penyebab kemungkinan terjadinya kegagalan akan menghasilkan mode kegagalan yang menyebabkan akibat tertentu. Berikut ini adalah ukuran parameter dari *occurance* [20].

Tabel 2. 4 Parameter Occurance

Occurence		*Rank*	*Criteria*
Extremely unlikely	*Failure occurs every 5 years*	*1*	*Failure highly unlikely*
Remote likelihood	*Failure occurs every 2 years*	*2*	*Rare number of failures likely*
Very low likelihood	*Failure occurs every year*	*3*	*Very few failure likely*
Low likelihood	*Failure occurs every 6 months*	*4*	*Few failures likely*
Moderately low likelihood	*Failure occurs every 3 months*	*5*	*Occasional failures likely*
Medium likelihood	*Failure occurs every month*	*6*	*Medium number of failures likely*

Occurence		*Rank*	*Criteria*
Medium high likelihood	*Failure occurs every week*	*7*	*Moderately high number of failures likely*
High likelihood	*Failure occurs every day*	*8*	*High number of failures likely*
Very high likelihood	*Failure occurs every shift*	*9*	*Very high number of failures likely*
Extremely likely	*Failure occurs every hour*	*10*	*Failure almost certain*

c) D = *Detection* (deteksi) / *Cause*

Detection atau sejauh mana peluang potensi kegagalan tersebut dapat teridentifikasi merupakan pengukuran dalam memperkirakan subjektif numerik dari kontrol untuk mencegah atau mendeteksi penyebab kegagalan sebelum kegagalan mencapai pengguna akhir atau pelanggan. Berikut ini adalah ukuran parameter dari *detection* [20].

Tabel 2. 5 Parameter Detection

Detection	*Rank*	*Criteria*
Extremely likely	*1*	*Can be corrected prior to engineering prototype*
Very high likelihood	*2*	*Can be detected and corrected prior to engineering design release*
High likelihood	*3*	*Has high effectiveness*
Moderately high likelihood	*4*	*Has moderately high effectiveness*
Medium likelihood	*5*	*Has medium effectiveness*

Detection	*Rank*	*Criteria*
Moderately low likelihood	*6*	*Has moderately low effectiveness*
Low likelihood	*7*	*Has low effectiveness*
Very low likelihood	*8*	*Has lowest effectiveness in each applicable category*
Remote likelihood	*9*	*Is unproven, unreliable or unknown*
Extremely unlikely	*10*	*No design technique available or known, and/or none is planned*

d) ***Risk Priority Number* (RPN)**

RPN adalah hasil ukuran yang digunakan untuk membantu mengidentifikasi mode kegagalan kritis terkait dengan suatu sistem yang mencakup desain atau proses. Nilai RPN berkisar dari 1 (terbaik) hingga 1000 (terburuk). Berikut ini merupakan penggambaran dari proses pembobotan faktor yang membentuk RPN.

$$\boldsymbol{RPN = S\ x\ O\ x\ D}$$

Keterangan:

S : *Severity number*
O : *Occurance number*
D : *Detection number*

Nilai RPN ini digunakan sebagai acuan untuk mengetahui mode kegagalan yang paling signifikan dalam memerlukan perbaikan. Setelah dilakukan perhitungan RPN untuk masing-masing potensi kegagalan, maka dapat disusun prioritas tindakan perbaikan berdasarkan nilai tersebut. Nilai RPN tersebut kemudian diklasifikasikan berdasarkan level prioritas kegagalan yang memerlukan penanganan lanjut. Nilai RPN yang paling tinggi menunjukkan

kegagalan yang memiliki prioritas penanganan lebih baik. Level prioritas kegagalan tersebut adalah sebagai berikut.

Tabel 2. 6 Level Prioritas Nilai RPN

RPN Calculation	Level
< 20	Very Low
< 80	Low
< 120	Medium
< 200	High
>200	Very High

Dalam penelitian ini, metode *FMEA* digunakan dalam penilaian risiko aset informasi sehingga didapatkan prioritas level risiko mulai dari level *very low* hingga *very high*

Sebagai contoh penilaian risiko dengan metode FMEA ini dapat dilihat pada gambar 2.4 di bawah ini.

No	Environment	Risk Event	Potential Causes	OCC	Alasan Penilaian Occurrence	Impact	SEV	Alasan Penilaian Severity	Current Control	DET	RPN	Status
RN-003	Network	Gangguan pada penyedia layanan	Penggunaan layanan jaringan pada jalur yang sama	3	Risiko ini jarang terjadi karena penyedia layanan yang handal	Sistem kredit tidak bisa diakses atau digunakan	7	Jika sistem tidak dapat digunakan, maka porses bisnis perusahaan akan terhenti, sehingga akan mengakibatkan kekecewaan pada pelanggan yang ingin melakukan proses peminjaman	-	10	210	Very High
RS-007	Software	Data hilang	Microsoft word dan excel crash	4	Risiko ini masih dikategorikan jarang ditemui karena selama ini sistem berjalan dg baik	Proses layanan kredit terhambat	5	Jika perangkat lunak mengalami error atau bug sehingga tidak dapat digunakan, maka porses bisnis perusahaan akan terhenti, sehingga akan mengakibatkan kekecewaan pada pelanggan yang ingin melakukan proses peminjaman	-	10	200	High
RN-001	Network	Kabel tercabut tanpa sengaja	Penempatan kabel jaringan yang tidak baik	5	Risiko ini beberapa kali ditemui karena kabel putus bisa karena penempatan kabel yang masih kurang tertata baik	Proses layanan kredit terhambat	8	Ketika kabel tercabut maka sistem akan menjadi tidak dapat digunakan	Memperbaiki penataan kabel jaringan secara rutin	5	200	High

Gambar 2. 4 Contoh Penilaian dengan Metode FMEA

2.6. *Information Secutity Management System* (ISMS)

Menurut McLeod Informasi didefinisikan sebagai data yang sudah diproses ataupun data yang memiliki arti. Informasi dibentuk dari gabungan data yang diharapkan memiliki arti untuk penerima.. Menurut ISO/IEC 17799:2005 mengenai information security management system menjelaskan keamanan informasi merupakan upaya untuk melindungi dari berbagai ancaman untuk memastikan kelanjutan bisnis, mengurangi resiko bisnis, serta meningkatkan investasi dan peluang bisnis yang ada.

International Organization for Standardization (ISO) atau yang biasa disebut sebagai Organisasi International untuk Standarisasi sudah membuat dan mengembangkan sejumlah standar mengenai Information Security Management Systems (ISMS) atau yang disebut Sistem Manajemen Keamanan Informasi (SMKI) mulai berupa persyaratan hingga panduan sejak tahun 2005. Secara umum, arti dari sebuah Sistem Manajemen Keamanan Informasi adalah sebuah prosedur yang ada dalam memanajemen keamanan informasi dengan tujuan agar terhindar dari berbagai resiko negatif.

ISMS Dikelompokkan sebagai seri / rangkaian dari ISO 27000, berikut ini adalah pembagian kelompok dari standar ISMS :

- ISO/IEC 27000:2009 – ISMS Overview and Vocabulary
- ISO/IEC 27001:2005 – ISMS Requirements
- ISO/IEC 27002:2005– Code of Practice for ISMS
- ISO/IEC 27003:2010 – ISMS Implementation Guidance
- ISO/IEC 27004:2009 – ISMS Measurements
- ISO/IEC 27005:2008 – Information Security Risk Management
- ISO/IEC 27006: 2007 – ISMS Certification Body Requirements
- ISO/IEC 27007 – Guidelines for ISMS Auditing

Pada penelitian ini penulis hanya akan berfokus pada seri ISO 27002 saja karena ISO 27002 menjelaskan mengenai praktek keamanan informasi beserta kendali tujuan secara rinci.

2.7. ISO 27002 Klausul Keamanan Fisik dan Lingkungan

ISO 27002 mempunyai beberapa *controls* dan *objective*. Berikut ini daftar *controls* dan *Obejctives* pada klausul Keamanan Fisik dan Lingkungan yang dipaparkan pada ISO 27002 [21]:

Tabel 2. 7 Control Objective ISO 27002 Klausul Keamanan Fisik dan Lingkungan

Poin Utama	*Control Objective*	Penjelasan
11.1 Secure areas		Untuk mencegah akses fisik oleh pihak yang tidak berwenang, kerusa-kan dan interferensi terhadap lokasi dan informasi organisasi.
	11.1.1 Physical security perimeter	Perimeter keamanan (batasan seperti dinding, pintu masuk yang dikendalikan dengan kartu atau meja resepsionis yang dijaga) harus digunakan untuk melindungi area yang berisi informasi dan fasilitas pengolahan informasi.
	11.1.2 Physical entry controls	Area yang aman harus dilindungi dengan pengendalian entri yang sesuai untuk memastikan

Poin Utama	*Control Objective*	Penjelasan
		bahwa hanya personel yang berwenang diperbolehkan untuk mengakses
	11.1.3 Securing offices, rooms and facilities	Keamanan fisik untuk kantor, ruangan dan fasilitas harus dirancang dan diterapkan.
	11.1.4 Protecting against external and environmental threats	Perlindungan fisik terhadap kerusakan akibat dari kebakaran, banjir, gempa bumi, ledakan, kerusuhan dan bentuk lain bencana alam atau buatan manusia harus dirancang dan diterapkan.
	11.1.5 Working in secure areas	Perlindungan fisik dan pedoman kerja dalam area yang aman harus dirancang dan diterapkan.
	11.1.6 Public access, delivery and loading areas	Titik akses seperti area bongkar muat dan titik lainnya dimana orang yang tidak berwenang dapat masuk kedalam lokasi harus dikendalikan dan, jika mungkin, dipisahkan dari fasilitas pengolahan informasi untuk mencegah akses yang tidak berwenang.
11.2 Equipment security		Untuk mencegah kehilangan, kerusakan, pencurian atau gangguan aset dan interupsi terhadap kegiatan organisasi

Poin Utama	*Control Objective*	Penjelasan
	11.2.1 Equipment siting and protection	Peralatan harus ditempatkan atau dilindungi untuk mengurangi risiko dari ancaman dan bahaya lingkungan dan peluang untuk akses oleh pihak yang tidak berwenang.
	11.2.2 Supporting utilities	Peralatan harus dilindungi dari kegagalan catu daya dan gangguan lain yang disebabkan oleh kegagalan sarana pendukung.
	11.2.3 Cabling security	Kabel daya dan telekomunikasi yang membawa data atau jasa informasi pendukung harus dilindungi dari intersepsi atau kerusakan.
	11.2.4 Equipment maintenance	Peralatan harus dipelihara dengan benar untuk memastikan ketersediaan dan integritasnya.
	11.2.5 Removal of property	Peralatan, informasi atau perangkat lunak tidak boleh dibawa keluar lokasi tanpa ijin yang berwenang.
	11.2.6 Security of equipment off premises	Keamanan harus diterapkan pada peralatan di luar lokasi dengan mempertimbangkan risiko yang berbeda pada saat bekerja di luar lokasi organisasi.
	11.2.7	Seluruh item atau peralatan yang memuat

Poin Utama	*Control Objective*	Penjelasan
	Secure disposal or re-use of equipment	media penyimpanan harus diperiksa untuk memastikan bahwa setiap data sensitif dan perangkat lunak berlisensi telah dihapus atau ditimpa (overwritten) secara aman sebelum dibuang.
	11.2.8 Unattended User Equipment	Peralatan yang ditinggalkan oleh penggunanya (unattended) harus dipastikan terlindungi dengan tepat.
	11.2.9 Clear desk and clear screen policy	Kebijakan clear desk terhadap kertas dan media penyimpanan yang dapat dipindahkan dan kebijakan clear screen untuk fasilitas pengolahan informasi harus ditetapkan.

Dalam penelitian ini, ISO 27002:2013 akan digunakan sebagai acuan untuk membuat prosedur audit program. Risiko yang telah dianalisis sebelumnya akan dipetakan pada ISO/IEC 27002:2013 ini sehingga akan didapatkan kendali tujuan mana sajakah yang berkaitan dengan lingkungan kerja di Direktorat Sistem Informasi (DSI) Universitas Airlangga. Hasil pemetaan ini nantinya akan dibuatkan prosedur program audit.

Halaman ini sengaja dikosongkan

BAB III
METODOLOGI PENELITIAN

Dalam melaksanakan pengerjaan Tugas Akhir maka diperlukan adanya metode pengerjaan dan jadwal rencana pelaksanaan.

3.1 Tahapan Pelaksanaan Penelitian

Pengerjaan tugas akhir ini akan melalui beberapa metode yang meliputi tahap perancangan, tahap implementasi, dan tahap pembahasan hasil. Pada bab ini akan dijelaskan secara detail masing-masing tahapan yang akan dilewati penulis seperti telah disebutkan di atas mengacu pada ISO/IEC 19011. Urutan dari metodologi ini ditunjukkan oleh Gambar 3.1.

Bahan dan peralatan yang digunakan dalam penelitian :
Bahan : ISO 27002:2013; ISO 19011
Peralatan : Google Drive, Microsoft Excel, Microsoft Project

3.1.1. Tahap Perancangan

Tahap pertama merupakan tahap perancangan. Tahap ini harus dilakukan guna mendapat informasi yang akan digunakan untuk menyusun dokumen panduan audit. Proses untuk tahapan persiapan ini dibagi menjadi dua, yaitu:

1) **Pengumpulan informasi organisasi** merupakan proses pertama untuk tahap persiapan guna mendapatkan informasi mengenai kondisi organisasi sehingga penulis **memperoleh gambaran kondisi Direktorat Sistem Informasi (DSI) Universitas Airlangga** saat ini. Pengumpulan data dan informasi DSI Universitas Airlangga yang dibutuhkan dilakukan dengan **dua cara**, yaitu:

a. Wawancara
   Wawancara dilakukan secara langsung kepada Direktur Sistem Informasi dan masing-masing Kasubbag. Dengan metode ini diharapkan dapat diperoleh kondisi kekinian Direktorat Sistem Informasi Universitas Airlangga terutama berkaitan dengan keamanan fisik dan lingkungan kerja.

b. Observasi
   Observasi merupakan salah satu pengumpulan data dengan mengadakan pengamatan langsung terhadap suatu objek pada periode tertentu. Pada penelitian ini observasi dilakukan dengan cara melakukan pengamatan secara langsung terhadap proses manajemen keamanan informasi di Direktorat Sistem Informasi Universitas Airlangga.

2) **Penentuan objek penelitian** adalah proses selanjutnya pertama untuk tahap perancangan. Pada tahap ini penulis akan menggunakan output dari proses sebelumnya, yaitu **gambaran kondisi Direktorat Sistem Informasi (DSI) Universitas Airlangga** dan akan diproses dengan cara **wawancara** dengan sub bagian keamanan informasi dan Direktur Sistem Informasi mengenai daerah kerja manakah yang paling rawan terhadap gangguan kemanan di lingkungan DSI Unair untuk dapat menentukan **bagian mana yang paling penting** untuk dibuatkan panduan audit.

3.1.2. Tahap Implementasi

Tahap implementasi ini merupakan tahap kedua yang berisi 6 proses yaitu:

1) **Penyusunan dokumen *audit plan*** yang merupakan proses pertama pada tahap ini, penulis mulai menyusun dokumen panduan audit TI dengan menggunakan data **kondisi**

organisasi dan fokus penelitian di tahap awal ditambah dengan **informasi mengenai proses audit dari ISO 19011** terkait audit ini.

Dokumen *audit plan* berisikan 3 bagian besar yaitu:

a. Informasi umum yang berisikan tujuan, ruang lingkup, referensi proyek, singkatan dalam audit, dan kontak auditor serta *auditee*
b. Proses Audit, berisikan tipe audit internal, subjek, peran dan tanggug jawab auditor, metode audit, serta jadwal pelaksanaan audit.

Dalam penyusunan dokumen *audit plan* ini penulis melakukan **wawancara** dengan pihak DSI Unair terkait dengan informasi *auditee* dan auditor. Selain itu akan dipastikan juga berapa lama audit akan berlangsung. Untuk bagian lain, seperti peran dan tanggung jawab, metode yang digunakan dan tipe audit yang digunakan didapatkan dari mengkaji dokumen lain yang terkait seperti ISO 19011.

2) **Verifikasi dokumen *audit plan*** merupakaan tahap selanjutnya dimana penulis akan menggunakan dokumen *audit plan* yang telah disusun pada tahap sebelumnya kepada pihak DSI Unair. Verifikasi ini bertujuan untuk mengetahui apakah setiap poin yang telah disusun di dalam *audit plan* sudah benar. Verifikasi yang dilakukan dengan pihak DSI Unair adalah yang terkait dengan informasi yang diminta dari pihak DSI Unair, sedangkan untuk poin lainnya yang terdapat pada *audit plan* seperti peran dan tanggung jawab auditor dan *auditee* akan ditinjau ulang dengan dokumen lain yang terkait.

Apabila dalam proses verifikasi ini masih ada kesalahan maka penulis akan memperbaiki dokumen dengan mengulang proses sebelumnya hingga dokumen audit plan ini disetujui oleh pihak DSI Unair.

3) **Identifikasi aset informasi**. Penulis melakukan identifikasi aset informasi yang terkait dengan klausul keamanan fisik dan lingkungan. Proses ini dilakukan dengan menggunakan informasi **ruang lingkup** yang ada di dalam *audit plan* dan metode **wawancara** dengan pihak terkait yaitu pihak keamanan data di Direktorat Sistem Informasi Universitas Airlangga mengenai aset apa sajakah yang dimiliki dan digunakan dalam proses bisnis. Pada tahapan ini akan diperoleh data mengenai aset informasi terutama yang terkait dengan klausul keamanan fisik dan lingkungandi ruang kerja yang ditentukan pada proses 2 yang ditulis dalam ***asset register*** yang akan digunakan sebagai masukan di proses berikutnya.

4) **Penilaian risiko TI menggunakan FMEA** merupakan proses ketiga untuk tahap implementasi. Penulis menggunakan ***asset register*** yang didapatkan dari proses sebelumnya dan melakukan identifikasi risiko TI terhadap aset yang dimiliki.Proses identifikasi risiko ini selanjutnya akan dinilai dengan menggunakan metode **FMEA** yang mempertimbangkan 3 hal yaitu *severity, occurrence,* dan *detection* pada setiap aset yang dimiliki. Selanjutnya risiko yang ada dikelompokkan menurut peringkat risikonya. Proses ini dapat menghasilkan daftar risiko yang tertuang dalam ***risk register***.

5) **Pemetaan risiko** merupakan proses selanjutnya pada tahap ini dimana penulis melakukan proses **pemetaan** risiko yang didapat dari proses sebelumnya, yaitu dari ***risk register***, ke dalam *control objective* yang dimiliki oleh ISO/IEC 27002:2013 khususnya klausul kemanan fisik dan lingkungan. Pemetaan harus dilakukan dengan seksama sehingga dokumen panduan audit dapat tepat sasaran. Proses ini pada akhirnya akan menghasilkan **risiko yang telah terpetakan** dalam *control objective* ISO/IEC 27002:2013.

6) **Penyusunan dokumen *audit program*** yang merupakan proses terakhir pada tahap ini, penulis mulai menyusun dokumen panduan audit TI dengan menggunakan data **risiko yang telah terpetakan** di proses sebelumnya serta dokumen *audit plan*.

   Dokumen Audit Program berisi tujuan dan ruang lingkup audit, kendali tujuan yang digunakan, prosedur program audit, dan dokumen kerja audit.
   Bagian kendali tujuan yang digunakan didapatkan dari pemetaan risiko dengan ISO/IEC 27002:2013, dengan cara mendaftar seluruh kendali tujuan yang punya pemetaan terhadap risiko yang ada.

   Bagian prosedur program audit/*checklist* audit berisikan prosedur untuk setiap kontrolnya dan daftar cek yang diperlukan. Sebagai contoh, untuk kontrol penghancuran atau pembuangan media terdapat prosedur pengecekan dokumen yang berisi mengenai setiap detail aktifitas penghancuran atau pembuangan media milik organisasi terdapat kontrol cek yang berupa dokumen log penghancuran media sensitif organisasi.

   Selain itu terdapat juga panduan penggunaan dokumen *audit program*, yang berisikan cara-cara menggunakan prosedur audit.

3.1.3. Tahap Pembahasan Hasil

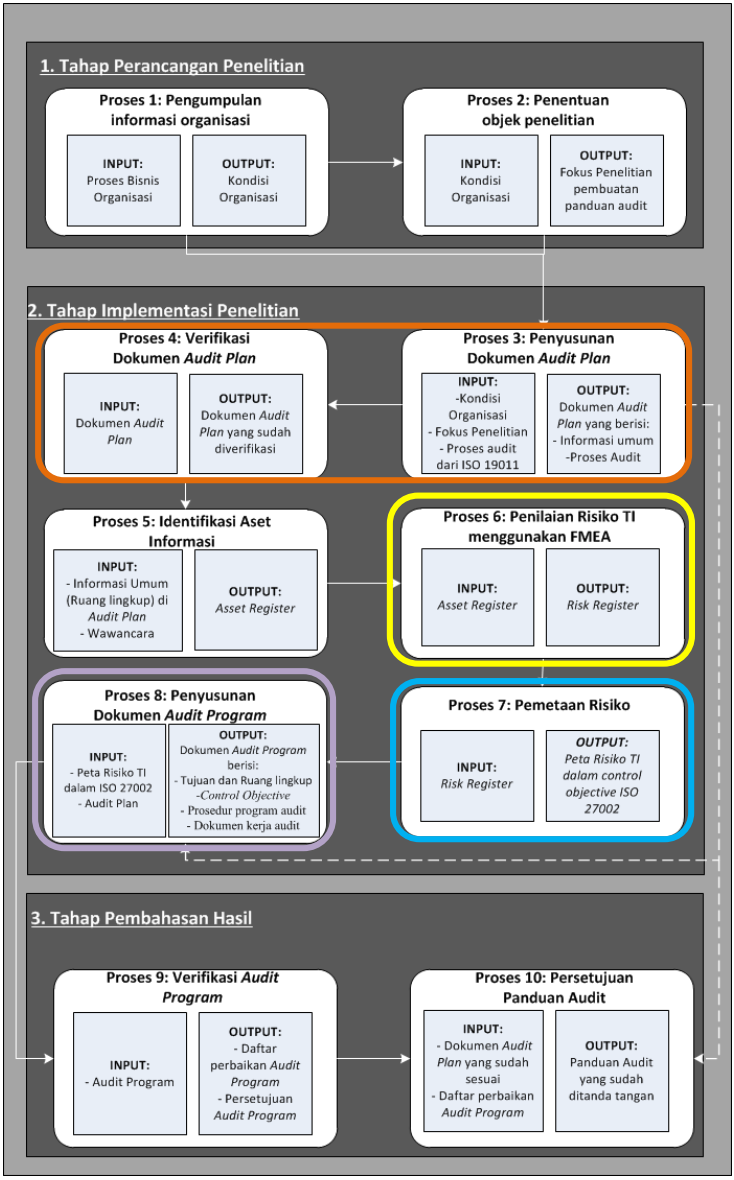
Pada tahapan ini, merupakan proses verifikasi dokumen panduan audit kepada kendali tujuan di ISO/IEC27002:2013 dan proses persetujuan dokumen panduan audit oleh pihak DSI Universitas Airlangga

1) **Verifikasi dokumen *audit program*** merupakan proses pertama pada tahap ini. Penulis akan **melakukan verifikasi**

dari pihak Direktorat Sistem Informasi serta *trace back* dengan standar yang digunakan yaitu ISO/IEC 27002:2013 terkait dokumen *audit program* yang telah dibuat. Verifikasi yang dilakukan adalah **pengecekan** apakah dokumen *audit program* khususnya prosedur audit tersebut **telah sesuai dengan standar ISO/IEC 27002:2013** serta mengecek kesesuaian informasi dengan tahap-tahap sebelumnya.

2) **Persetujuan dokumen Panduan Audit** merupakan proses terakhir dari tahap ini dan keseluruhan metodologi dimana penulis melakukan **proses persetujuan** terhadap dokumen *panduan audit* yang telah dibuat. Dokumen *audit plan* yang telah dibuat dan *audit program* akan **ditandatangani** dan siap digunakan oleh Direktorat Sistem Informasi.

Keterangan Gambar 3.1:
Rumusan Masalah 1
Rumusan Masalah 2
Rumusan Masalah 3
Rumusan Masalah 4



Gambar 3. 1 Metodologi Peneliti

Halaman ini sengaja dikosongkan

BAB IV
PERANCANGAN

Bagian ini menjelaskan perancangan penelitian tugas akhir. Perancangan ini diperlukan sebagai panduan dalam melakukan penelitian tugas akhir.

4.1 Perancangan Studi Kasus

4.1.1 Tujuan Studi Kasus

Penggunaan studi kasus merupakan suatu hal penting di dalam suatu penelitian. Pentingnya penggunaan sebuah studi kasus menurut para ahli yaitu:

1. Studi kasus dalam penelitian merupakan sebuah aktivitas pengamatan yang berfokus untuk mendeskripsikan, memahami, memprediksi ataupun mengontrol sebuah individu [22].
2. Sykes (1990) mengatakan bahwa tidak mudah dalam mendapatkan jenis-jenis informasi tertentu yang sulit bahkan tidak mungkin untuk didapatkan selain dengan menggunakan studi kasus [23].
3. Yin (2003) mengatakan sebuah studi kasus adalah suatu metode unik untuk mengamati sebuah topik empiris yang dilakukan berdasarkan satu set prosedur yang telah dibuat sebelumnya. Studi kasus merupakan cara yang unik untuk mengamati fenomena alam yang ada pada sekumpulan data. [24].
4. Miles & Huberman menyatakan sebuah studi kasus merupakan suatu kerangka kerja sistematis untuk melakukan sebuah penelitian. Penggambarkan sebuah fenomena yang terjadi berdasarkan tujuan penelitian yang konteknya dibatasi berdasarkan sebuah kerangka kerja juga dapat dilakukan dengan bantuan studi kasus. [25]

Terdapat tiga kategori studi kasus sebagaimana yang dikemukakan oleh Yin [24], yaitu:

1. Studi kasus eksplorasi *(exploratory)* bertujuan untuk menggali fenomena dalam data yang berfungsi sebagai tempat tujuan peneliti.
2. Studi kasus deskriptif *(descriptive)* bertujuan untuk menggambarkan fenomena alamiah yang terjadi dalam data.
3. Studi kasus *explanatory,* bertujuan untuk menjelaskan fenomena dalam data secara detail mulai dari hal yang dasar samapi dalam.

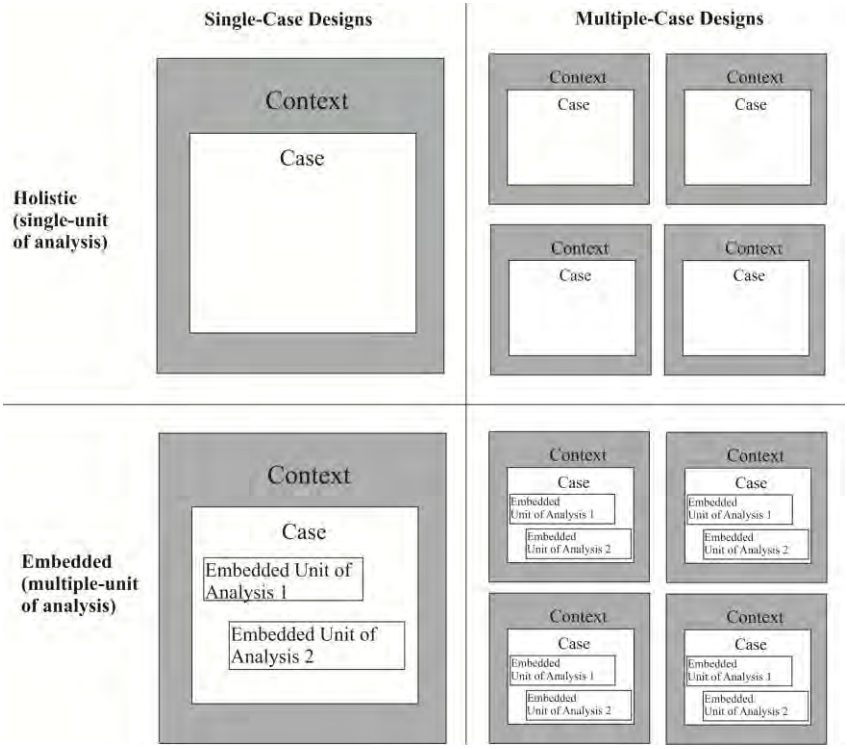
Pengerjaan penelitian ini dirancang dengan menggunakan studi kasus. Penggunaan studi kasus dalam pengerjaan penelitian ini adalah untuk melakukan eksplorasi suatu permasalahan lebih mendalam lagi. Harapan peneliti dengan menggunakan studi kasus adalah untuk mempermudah penggalian informasi dan penerapan data yang didapatkan selama penelitian.

Menurut Yin langkah selanjutnya yang dapat dilakukan adalah dengan melakukan perancangan penelitian merupakan langkah berikutnya setelah melakukan pemilihan penggunaan studi kasus. Tahap perancangan akan membantu penulis dalam menentukan dan memahami tujuan pemilihan studi kasus, persiapan pengumpulan data untuk kebutuhan penelitian, menentukan metode pengolahan data hingga menentukan pendekatan untuk melakukan analisis mendalam mengenai data yang nantinya akan digunakan selama proses penelitian. [24]

4.1.2 Unit of Analysis

Yin [24] menjelaskan bahwa dalam memilih studi kasus terdapat dua tipe yaitu *single-case design* dan *multiple-case design*. *Single-case design* menekankan peneliti untuk lebih perhatian terhadap kasus dan lebih fokus terhadap metode yang digunakan di dalamnya. *Single-case design* menggunakan satu studik kasus yang unik, kritis dengan mengamati dan mengeksplorasi kondisi tertentu pada suatu kasus untuk menguji kebenaran suatu teori [26] [27]. Tipe yang kedua adalah *multiple-case design* yang menggunakan lebih dari satu

studi kasus bertujuan untuk membandingkan beberapa studi kasus yang ada dan bertujuan untuk melakukan replikasi temuan di seluruh studi kasus [28]. Perbedaan mendasar kedua tipe ini terletak pada jumlah *unit of analysis* yang digunakan seperti yang dapat terlihat pada Gambar 4.1.



Gambar 4. 1 Hubungan Unit of Analysis dengan Tipe Studi Kasus [28]

Dalam penelitian ini penulis menggunakan *single-case design* dengan satu *unit of analysis*. Pemilihan jenis studi kasus ini karena penulis akan mengeksplorasi sebuah permasalahan dalam sebuah studi kasus yaitu penyususnan dokumen paanduan audit pada sebuah organisasi.

4.2 Persiapan Pengumpulan Data

Tahapan selanjutnya pada tahapan perancangan adalah persiapan pengumpulan data. Said (2015) mengatakan dalam artikelnya, teknik pengumpulan data pada penelitian terdapat 5 teknik diantaranya adalah kuesioner, tes, wawancara, dokumen, dan observasi [29]. Beberapa metode di atas akan digunakan dalam jangka waktu tertentu selama proses penelitian berlangsung sesuai dengan kerangka kerja yang diterapkan pada studi kasus untuk mencapai suatu tujuan yang diinginkan.

Metode untuk mengumpulkan data yang dibutuhkan peneliti akan melakukan beberapa metode diantaranya adalah wawancara dan observasi. Dalam kegiatan wawancara akan dilakukan pada orang-orang yang berhubungan dengan keamanan informasi di area DSI Unair, antara lain kasubdit keamanan data dan kasubbag keamanan jaringan. Wawancara ini dilakukan untuk mendapatkan informasi mengenai kondisi kekinian, risiko yang dimiliki, dan audit yang pernah dilakukan. Teknik yang kedua adalah dengan melakukan observasi terhadap kondisi di area server DSI guna mengetahui bagaimana pengelolaan keamanan fisik dan lingkungan TI di area DSI. Dari dua teknik pengumpulan data yang akan dilakukan dalam penelitian ini, berikut beberapa detail data yang ingin di dapatkan selama proses penelitian:

1. Tugas pokok divisi DSI.
2. Kondisi kekinian manajemen keamanan fisik dan lingkungan TI yang bisa di dapatkan dengan melakukan observasi, dan wawancara.
3. Audit keamanan fisik dan lingkungan TI yang pernah dilakukan sebelumnya.
4. Aset-aset teknologi informasi terkait dengan ruang kerja DSI dan kemanan fisik dan lingkungan TI.

4.3 Metode Pengolahan Data

Metode pengolahan data pada penelitian ini terdapat dua metode yang digunakan. Metode pertama dilakukan agar penulis dapat dengan mudah melakukan analisis pada hasil wawancara dengan pihak-pihak terkait, yaitu dengan melakukan penulisan ulang hasil rekaman wawancara pada recorder menggunakan tools *Microsoft Word*. Untuk metode yang kedua yaitu dengan melakukan pengolahan data untuk memberikan penilaian-penilaian terhadap asset-aset terkait keamanan fisik dan lingkuangan. Penilaian-penilaian ini digunakan untuk melakukan prioritisasi terhadap risiko berdasarkan metode FMEA dengan aspek-aspek *Severity Number* (SEV) dan *Probability Number* (OCC).

4.4 Pendekatan Analisis

Analisis terhadap data perlu dilakukan setelah melakukan pengumpulan data. Hal ini dilakukan untuk mengetahui hubungan antara data dengan objek yang diinginkan. Beberapa pendekatan analisis yang akan dilakukan antara lain adalah:

1. **Analisis dengan pendekatan konseptual**
   Analisis ini dilakukan dengan analisis tugas pokok dan fungsi (tupoksi) yang ada di bagian DSI guna mengetahui tugas masing-masing staff. Selain itu akan dilakukan analisis kondisi kekinian terhadap keamanan fisik dan lingkungan, yang mana nantinya akan dipetakan dalam standar ISO/IEC 27002:2013.

2. **Analisis dengan pendekatan standar**
   a. PMBOK – *Project Plan*
      Analisis dengan PMBOK pada proses *Project Plan* digunakan untuk menganalisis hal yang diperlukan saat akan menyusun dokumen *audit plan.*

b. PMBOK – *Project Program*
   Analisis dengan PMBOK pada proses *Project Program* digunakan untuk menganalisis hal yang diperlukan saat akan menyusun dokumen *audit program.*
c. ISO/IEC 27002:2013 – Keamanan Fisik dan Lingkungan TI
   Analisis dengan ISO/IEC 27002:2013 pada klausul keamanan fisik dan lingkungan digunakan untuk mengetahui praktik keamanan fisik dan lingkungan yang sesuai dengan standar.

BAB V
IMPLEMENTASI

Bab ini menjelaskan tentang implementasi setiap tahap dan proses-proses di dalam metodologi pengerjaan tugas akhir, yang dapat berupa hasil, waktu pelaksanaan dan lampiran terkait yang memuat pencatatan tertentu terhadap kondisi pengimplementasi proses itu sendiri.

5.1. Analisis Kondisi Kekinian Organisasi

Pada poin ini akan dijelaskan hasil dari analisis yang dilakukan melalui metode observasi dan wawancara dengan pihak Direkotorat Sistem informasi Universitas Airlangga (DSI UA).

5.1.1. Gambaran Umum Direktorat Sistem Informasi Universitas Airlangga

Direktorat Sistem Informasi adalah suatu Direktorat dimana mengemban tugas sebagai pengembang sistem informasi dan memberikan layanan dukungan dalam bidang teknologi informasi bagi civitas akademika Universitas Airlangga.Pengelolaan sistem informasi Universitas Airlangga berada di bawah tanggung jawab langsung Wakil Rektor III. Direktorat Sistem Informasi (DSI) mendukung tugas pokok dan fungsi Wakil Rektor III di bidang Sistem Informasi. Sedangkan dalam pelaksanaan pengelolaan dan pengembangan sistem informasi Universitas Airlangga dilakukan oleh Direktorat Sistem Informasi. Pada tingkat fakultas pengelolaan dilakukan oleh Unit Sistem Informasi dengan penentu kebijakan operasionalnya adalah Wakil Dekan III.

Dalam operasional sehari-hari Direktorat Sistem Informasi adalah memberikan layanan internal dan eksternal dalam program pendidikan seperti sistem ERP Cybercampus, membangun website untuk kegiatan pendidikan serta proses belajar mengajar yang didukung oleh infrastruktur teknologi informasi dan komunikasi yang mutakhir.Direktorat Sistem Informasi tidak memiliki wewenang dalam kebijakan

akademik, untuk kebijakan akademik terdapat satu Direktorat tersendiri di Universitas Airlangga yang dinamakan dengan Direktorat Pendidikan dan dibantu oleh pihak akademik fakultas masing-masing.

Fungsi dari Direktorat Sistem Informasi adalah mengembangkan sistem informasi guna mewujudkan sistem informasi manajemen yang mendukung kegiatan proses belajar mengajar dan akademik. Selain itu pula mengumpulkan serta mengolah data dan informasi dan menyajikan informasi. Memberikan dukungan teknis untuk membangun infrastruktur berbasis teknologi informasi termasuk didalamnya jaringan komputer baik *wired* ataupun *non wired*. Visi dan Misi Direktorat Sistem Informasi Universitas Airlangga

Visi

Sebagai bagian dari Universitas Airlangga, Direktorat Sistem Informasi (DSI) berusaha menunjang terealisasinya visi institusional Unair untuk menjadi Perguruan Tinggi yang mandiri, inovatif, terkemuka, pelopor pengembangan ilmu pengetahuan, teknologi, humaniora, dan seni, berdasarkan moral agama, melalui ketersediaan sistem dan teknologi informasi yang handal dan terpercaya.

Misi

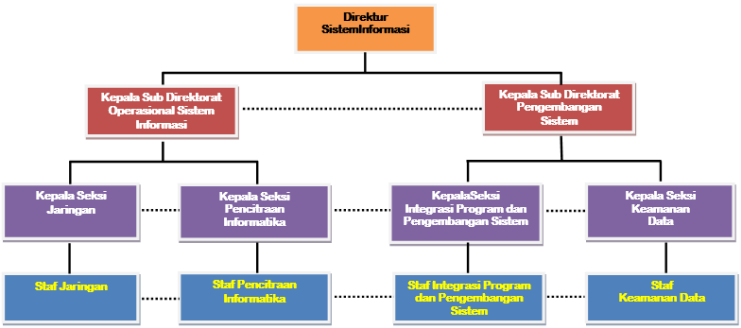
Memberi dukungan teknologi komunikasi dan informasi terhadap :

a. Penyelenggaraan pendidikan akademik, vokasional dan profesi.
b. Penyelenggaraan penelitian dasar, terapan dan penelitian kebijakan yang inovatif untuk menunjang pengembangan pendidikan dan pengabdian kepada masyarakat.
c. Dharmabakti keahlian dalam bidang ilmu, teknologi, humaniora dan seni kepada masyarakat.
d. Upaya kemandirian dalam pelaksanaan Tri Dharma Perguruan Tinggi melalui pengembangan kelembagaan

manajemen yang berorientasi pada mutu dan kemampuan bersaing secara internasional

5.1.2. Struktur Organisasi Direktorat Sistem Informasi

Direktorat Sistem informasi berada di bawah naungan Universitas Airlangga, namun untuk mendukung keberlangsungan bisnisnya, maka Direktorat Sistem Informasi memiliki struktur organisasi sendiri yang dibagi dalam beberapa seksi. Adanya seksi-seksi ini diharapkan mampu melaksanakan misi-misis DSI untuk mencapai visinya. Berikut ini adalah susunan organisasi di DSI:



Gambar 5. 1 Struktur Organisasi Direktorat Sistem Informasi

Pada Gambar 5.2 di atas ini terlihat terdapat 3 Ruang Lingkup Utama Proses Direktorat Sistem Informasi Universitas Airlangga yaitu Pendukungan, Pemrosesan dan Publikasi dan Didukung oleh pengaplikasian standard ISO 27001.

Gambar 5. 2 Diagram Kerja Direktorat Sistem Informasi

Berikut in rincian tugas pokok dan fungsi per seksi yang ada:

1. Network (warna biru) memiliki tugas pada bagian email, koneksi, dan server
2. Keamanan data (warna merah) memiliki tugas tentang keamanan data , pentest, risk assessment
3. Branding (warna ungu) memiliki tugas dalam hal pencitraan internal (tentang anggaran dan surat menyurat), pencitraan eksternal (webometric dan pemeringkatan perguruan tinggi lainnya), dan helpdesk.
4. SIAD (warna kuning) memiliki tugas dalam pengawalan dan pengembangan kolabirasi sistem (cyber campus) dan pengembangan aplikasi opsional (web official, web yang berkaitan dengan pengabdian masyarakat).

5.2. Penentuan Objek Penelitian

Setelah melakukan pengumpulan informasi mengenai kondisi organisasi, langkah selanjutnya adalah menentukan objek penelitian sebagai target panduan audit yang akan dibuat. Ruang kerja di Direktorat Sistem Informasi Universitas Airlangga dibagi dalam 3 lokasi, yaitu ruang kerja utama, ruang helpdesk dan ruang *data center*.

Hasil wawancara yang telah dilakukan, menunjukkan bahwa ruang *data center* atau ruang server merupakan daerah paling kritis karena dalam ruang server menyimpan data dari seluruh kampus A, B, dan C Universitas Airlangga. Maka dari itu, penulis memilih ruang server untuk dijadikan objek penelitian untuk mengetahui kekuatan keamanan yang ada di sana. Hasil dari wawancara dapat dilihat pada Lampiran A Tabel A.2.

5.3. Penyusunan Dokumen *Audit Plan* DSI Universitas Airlangga

5.3.1. Tujuan Dokumen *Audit Plan*

Tujuan dari pembuatan dokumen *audit plan* bagi Direktorat Sistem Informasi Universitas Airlangga sebagai berikut.

a. Menjadi panduan bagi auditor internal dalam melakukan proses audit yang mudah dipahami dan mudah diterapkan dengan tepat dan cepat.
b. Menjadi bahan pertimbangan bagi Direktorat Sistem Informasi untuk digunakan sebagai masukan untuk dokumen organisasi terutama yang terkait dengan audit TI.
c. Meningkatkan efektifitas dan efisiensi auditor dalam melakukan proses audit.

5.3.2. Penyusunan Bagian Informasi Umum

Dokumen *audit plan* didahului dengan informasi umum yang berisi informasi mengenai audit yang akan dilakukan. Pada bagian informasi umum terdiri dari informasi mengenai tujuan

audit plan, ruang lingkup audit plan, gambaran system yang akan diauidt, referensi dokumen, akronim dan singkatan yang digunakan dalam dokumen audit, serta kontak auditor dan auditee. Bagian tujuan, ruang lingkup, akronim dan singkatan berasal dari dokumen referensi lainnya yang berhubungan dengan dokumen audit plan yang kemudian disesuaikan dengan studi kasus tugas akhir. Sedangkan untuk gambaran sistem, referensi dokumen dan kontak auditor dan auditee didapatkan dari hasil interview penulis yang dapat dilihat pada Lampiran A Tabel A.2; A.3; dan A.4.

5.3.3. Penyusunan Bagian Proses Audit

Pada bagian proses audit secara garis besar berisi mengenai apa yang akan dan harus dilakukan pada saat proses audit berlangsung. Bagian ini terdapat beberapa sub-bagian yaitu tipe audit internal, subjek audit internal, peran dan tanggung jawab, dan metode audit internal yang didapatkan dari studi literature yang dilakukan oleh penulis, serta terdapat sub-bagian Jadwal kegiatan yang didapatkan dari ISO 19011 dan interview dengan pihak DSI Universitas Airlangga.

Sub-bagian jadwal audit menjelaskan mengenai aktivitas yang harus dilalui oleh tim audit sehingga audit akan dapat berjalan dengan baik. Sub-bagian aktivitas audit dibagi menjadi 3 bagian besar yaitu *preparation, execution,* dan *closing*. Pengkategorian aktivitas didasarkan pada referensi ISO 19011 yang digunakan oleh penulis. Waktu pelaksanaan audit didapatkan melalui pengembangan hasil interview yang menyatakan bahwa audit dilaksanakan pada akhir tahun dalam waktu kurang lebih 10 hari kerja.

Sedangkan untuk bagian lain, yaitu *Work Breakdown Structure (WBS), Gantt Chart,* dan *Milestone* merupakan penjabaran dari sub-bagian daftar aktivitas audit. WBS menggambarkan daftar aktivitas yang akan dilalui saat proses audit dalam bentuk bagan, sedangkan *Gantt chart* menunjukkan daftar aktivitas audit dalam bentuk grafik yang menggambarkan waktu

pelaksanaan. Sub-bagian *milestone* menyajikan informasi mengenai pencapaian dan hasil dari setiap aktivitas audit.

Contoh dari bagian ini dapat dilihat pada **Lampiran B**.

5.3.4. Penyusunan Bagian Evaluasi

Bagian audit plan ini berisi informasi mengenai strategi dan identifikasi risiko. Sub-bagian strategi berisi informasi mengenai saran dan kiat yang ditujukan untuk auditor sehingga kegiatan audit lebih terarah dan dapat mencapai tujuan yang diinginkan. Sub bagian ini didapatkan dari studi literatur yang dilakukan oleh penulis.

Sedangkan sub-bagian identifikasi risiko merupakan sub-bagian yang berisi mengenai risiko dalam melakukan proses audit. Sub-bagian ini bertujuan untuk membantu tim auditor untuk mempersiapkan diri dalam menghadapi risiko sehingga membantu dalam mengelola (*mitigate*) risiko lebih baik.

Seluruh dokumen audit plan dapat dilihat pada buku produk Dokumen Internal Audit Plan.

5.4. Verifikasi Dokumen *Audit Plan*

Pada poin ini akan dijelaskan mengenai verifikasi dokumen *Audit Plan*. Verifikasi yang dilakukan yaitu 2 hal. Pertama, verifikasi terhadap pihak DSI Universitas Airlangga. Verifikasi ini untuk mengetahui apakah informasi yang ada di dalam dokumen sudah benar, khususnya bagian 1, Informasi Umum. Verifikasi dilakukan dengan cara wawancara dengan pihak DSI sudah mengetahui isi dari *Audit plan* yang telah dibuat penulis. Hasil dari verifikasi adalah penulis mendapatkan perubahan informasi dari Kepala Seksi Keamanan Data mengenai informasi Auditor dan Auditee untuk keamanan fisik dan lingkungan di ruang server dan durasi aktivitas. Hasil Verifikasi dapat dilihat pada Tabel 5.1. Hasil wawancara dapat dilihat pada Lampiran A Tabel A.10.

Tabel 5. 1 Verifikasi Audit Plan dengan Organisasi

Susunan Dokumen		Check	Keterangan
Poin	Proses		
1.	Informasi Umum	x	Perbaikan pada bagian kontak auditor dan auditee
2.	Proses Audit	x	Pengurangan durasi audit
3.	Evaluasi	v	-

Untuk verifikasi kedua, dilakukan dengan mencocokkan aktivitas audit yang ada di Bagian 2 *Audit Plan* dengan proses audit yang ada di ISO 19011. Verifikasi kedua ini dilakukan dengan metode *traceback* dari dokumen yang telah penulis buat ke ISO 19011. Hasil verifikasi dapat dilihat pada Tabel 5.2.

Tabel 5. 2 Verifikasi Daftar Aktivitas Audit

Daftar Aktivitas		Standar ISO 19011		Check
Poin	Proses	Poin	Proses	
1.1.	Initiation	6.2	Initiating the audit	v
1.2.	Plannig	6.3	Preparing audit activities	v
3.0	Execution	6.4	Conducting the audit activities	v
4.0	Closing	6.5	Preparing and distributing audit report	v

5.5. Identifikasi Aset Ruang Server Direktorat Sistem Informasi

Pusat data atau ruang server Direktorat Sistem Informasi merupakan sebuah tempat yang berfungsi sebgai tempat pengolahan informasi seluruh Universitas Airlangga yang

terdiri dari perangkat keras (*hardware*), perangkat lunak (*software*), database, dan fasilitas pendukung lainnya. Pengelolaan ruang server merupakan tanggung jawab dari seksi jaringan.

Pada tugas akhir kali ini, aset yang diteliti hanya aset yang termasuk dalam *physical asset* yang terdiri dari perangkat keras, jaringan, dan manusia. Tabel 5.3 berikut ini merupakan data yang diperoleh mengenai daftar aset teknologi informasi yang dimiliki oleh ruang server DSI.

Tabel 5. 3 Daftar Aset Ruang Server Universitas Airlangga

No.	Kategori Aset	Jenis Aset
1.	Hardware	Server
2.		*Personal Computer (PC)*
3.		CPU
4.		UPS
5.		*Smoke detector*
6.		Alat pemadam kebakaran
7.		CCTV
8.		*Fingerprint*
9.		Sistem Pendingin (AC)
8.	Jaringan	Switch
9.		Firewall
10.		Hub
11.		Router
12.		Fiber optik
13.	Manusia	Pengelola (Staff seksi jaringan)

Untuk akses pengaman fisik di ruang server, terdapat sebuah pintu sebagai *single point of access* yang keamanannya merupakan tanggung jawab dari staff seksi jaringan di dalamnya. Namun pengelolaan *logbook* pengunjung belum dilakukan secara tepat. Hal ini terlihat saat penulis melakukan observasi tidak melakukan pencatatan walaupun tetap didampingi oleh staff yang berwenang.

5.6. Penilaian dan Analisis Risiko TI

Pada sub-bab ini akan dijelaskan mengenaik proses analisis risiko dan penilaian risiko berdasarkan metode FMEA. Keluaran untuk sub-bab ini adalah risiko TI yang mungkin terjadi, hasil penilaian risiko, dan urutan risiko dari nilai RPN yang tertinggi.

5.6.1. Pendefinisian TI untuk Risiko yang Dianalisis

Penilaian risiko TI yang dilakukan berfokus hanya pada 3 aset TI yang dimiliki oleh Direktorat Sistem Informasi Universitas Airlangga, yaitu aset *hardware, network,* dan *people*. Pemilihan asset TI yang akan dianalisis didasari pada aset yang berkaitan dengan keamanan fisik dan lingkungan TI, yaitu aset fisik. Sedangkan untuk *software* dan *data* tergolong dalam aset logis yang tidak berkaitan dengan keamanan fisik dan lingkungan TI.

5.6.2. Identifikasi Risiko

Tahapan awal dalam analisis risiko adalah identifikasi risiko-risiko yang mengancam aset TI Direktorat Sistem Informasi Universitas Airlangga. Risiko yang dimaksud di sini adalah sebuah kejadian yang memiliki kemungkinan terjadi di suatu hari yang disebabkan oleh faktor internal maupun eksternal organisasi dan memiliki dampak negatif bagi proses bisnis organisasi. Pada Tabel 5.4 diketahui bahwa ada sembilan kategori risiko yang teridentifikasi mengancam aset TI organisasi terkait dengan control kemanan fisik dan lingkungan TI.

Tabel 5. 4 Risiko aset TI

	Faktor	*Risk ID*	*Potential Risks*
Risiko Eksternal	Bencana	R-01	Bencana Alam
	Gangguan Fasilitas	R-02	Kebakaran
		R-03	Power Failure
	Kerjasama	R-04	Pelanggaran SLA
Risiko Internal	Operasional	R-05	Hardware Failure
		R-06	Network Failure
		R-07	Pencurian data fisik
		R-08	Human error
		R-09	Pelanggaran regulasi

5.6.3. Penilaian Risiko

Pada tahapan ini akan dilakukan penilaian secara kuantitatif terhadap sembilan risiko yang telah teridentifikasi dengan menggunakan metode FMEA. Penilaian risiko dengan metode FMEA ini mempertimbangkan tiga aspek untuk menghasilkan sebuah nilai yaitu penyebab terjadinya risiko, dampak yang ditimbulkan oleh risiko, dan kontrol yang telah dimiliki organisasi saat ini untuk mengatasi risiko yang ada. Perhitungan tiga aspek tersebut akan menghasilkan *Risk Priority Number* (RPN), dimana nanti RPN ini akan mengindikasikan sebuah risiko tergolong kategori *Very Low, Low, Medium, High,* atau *Very High*. Oleh karena itu, untuk mendapat hasil yang optimal dari hasil penilaian, risiko yang telah dianalisis sebelumnya dipecah berdasarkan penyebabnya dan dampaknya, baik terhadap aset TI maupun terhadap bisnis. Sehingga dari sembilan risiko yang telah dianalisis berkembang menjadi 34 risiko. Tabel 5.5 di bawah ini menunjukkan kemungkinan risiko beserta penyebabnya dan dampaknya.

Tabel 5. 5 *Risk Register*

Ketegori Asset	Asset	Penyebab	Risiko	Dampak terhadap Bisnis
Hardware	Genset	Genset tidak berfungsi ketika tenaga listrik DSI UA mengalami pemadaman	*Power Failure*	Proses bisnis yang bergantung pada koneksi internet terganggu, sehingga produktivitas menurun
Hardware	UPS	Kebakaran pada baterai UPS	Kebakaran	Proses bisnis terhenti jika terjadi pada jam kerja
Hardware	UPS	Kebakaran pada baterai UPS	Kebakaran	Proses bisnis yang bergantung pada koneksi internet terganggu, sehingga produktivitas menurun
Hardware	UPS	Kegagalan fungsi UPS untuk menyuplai listrik	*Power Failure*	Proses bisnis yang bergantung pada koneksi internet terganggu, sehingga produktivitas menurun

Ketegori Asset	Asset	Penyebab	Risiko	Dampak terhadap Bisnis
		karena kesalahan konfigurasi		
Hardware	Server	Petir, Angin kencang	Bencana Alam	Proses bisnis yang berkaitan dengan server yang rusak terhenti hingga server dapat pulih
Hardware	Server	Gempa Bumi	Bencana Alam	Proses bisnis terhenti
Hardware	Server	Kesalahan prosedur kerja	*Human error*	Proses bisnis yang berkaitan dengan server yang rusak terhenti hingga server dapat pulih
Hardware	Server	*Server Overload*	*Hardware Failure*	Proses bisnis yang berkaitan dengan server tersebut terganggu, sehingga produktivitas menurun

Ketegori Asset	Asset	Penyebab	Risiko	Dampak terhadap Bisnis
Hardware	*Personal Computer* (PC)	Proses *maintenance* aset tidak dilakukan dengan benar	*Hardware Failure*	Proses bisnis yang berkaitan dengan PC tersebut terganggu, sehingga produktivitas menurun
Hardware	*Smoke Detector*	Proses *maintenance smoke detector* tidak dilakukan dengan benar	*Hardware Failure*	Proses bisnis seluruhnya terhenti jika tidak dapat dipadamkan
Hardware	*Smoke Detector*	*Smoke detector* sudah usang	*Hardware Failure*	Proses bisnis seluruhnya terhenti jika tidak dapat dipadamkan
Hardware	Pendingin ruangan	Proses monitoring suhu ruangan data center tidak dilakukan dengan maksimal	Pelanggaran regulasi	Proses bisnis yang berkaitan dengan server yang rusak terhenti hingga server dapat pulih

Ketegori Asset	Asset	Penyebab	Risiko	Dampak terhadap Bisnis
Hardware	Perangkat Storage (Harddisk, Removable Media)	Kerusakan fisik	*Hardware Failure*	Sebagian proses bisnis yang terkait dengan data yang rusak terganggu, sehingga produktivitas menurun
Hardware	Perangkat Storage (Harddisk, Removable Media)	Aktivitas pembuangan media penyimpanan tidak sesuai prosedur	Pelanggaran regulasi	Menurunnya reputasi
Hardware	CCTV	Kesalahan pada tata letak CCTV	*Hardware Failure*	• Menurunnya reputasi • Proses bisnis terganggu
Hardware	Perangkat Penyimpanan dan penataan Server (rak,	Kesalahan pengaturan dan keamanan di ruang server	Pencurian data fisik	• Menurunnya reputasi • Proses bisnis terganggu

Ketegori Asset	Asset	Penyebab	Risiko	Dampak terhadap Bisnis
	lemari, soket)			
Hardware	Perangkat Listrik	Terjadi konsleting/hubungan arus pendek	*Power Failure*	Proses bisnis yang bergantung pada koneksi internet terganggu, sehingga produktivitas menurun
Hardware	Perangkat Listrik	Terjadi konsleting/hubungan arus pendek	Kebakaran	Proses bisnis akan terhenti
Hardware	Perangkat Listrik	Gangguan panel listrik	*Power Failure*	Proses bisnis yang bergantung pada koneksi internet terganggu, sehingga produktivitas menurun
Hardware	Perangkat Listrik	Gangguan panel listrik	Kebakaran	Proses bisnis akan terhenti

Ketegori Asset	Asset	Penyebab	Risiko	Dampak terhadap Bisnis
Hardware	Perangkat jaringan (Switch, Router)	Konfigurasi keamanan lemah	*Network Failure*	• Menurunnya reputasi • Proses bisnis terganggu
Hardware	HUB	Kesalahan konfigurasi	*Hardware Failure*	Proses bisnis terganggu
Hardware	Fingerprint	Sidik jari pegawai tidak terbaca	*Hardware Failure*	• Menurunnya reputasi • Proses bisnis terganggu
Hardware	Kabel Jaringan	Penempatan kabel jaringan yang tidak baik	*Network Failure*	Proses bisnis yang bergantung pada koneksi internet terganggu, sehingga produktivitas menurun
Network	Jaringan MPLS	Kurang monitoring dan review SLA	Pelanggaran SLA	Proses bisnis yang bergantung pada koneksi internet terganggu, sehingga produktivitas menurun

Ketegori Asset	Asset	Penyebab	Risiko	Dampak terhadap Bisnis
Network	Koneksi Internet	Kehilangan akses remote data ke server	*Network Failure*	Proses bisnis yang berkaitan dengan aplikasi tersebut terganggu
Network	Koneksi Internet	Kehilangan akses remote data ke server	*Network Failure*	• Menurunnya reputasi • Proses bisnis terganggu
People	Admin	Penyalahgunaan akses admin	Pelanggaran regulasi	• Menurunnya reputasi • Proses bisnis terganggu
People	Staff	Pemberian hak akses yang tidak sesuai prosedur	Pelanggaran regulasi	• Menurunnya reputasi • Proses bisnis terganggu
People	Staff	Kesalahan penggunaan akun	Pelanggaran regulasi	Proses bisnis terhambat
People	Staff	PC ditinggalkan dalam keadaan *log-in* tanpa adanya penjagaan	*Human error*	• Menurunnya reputasi • Proses bisnis terganggu

Ketegori Asset	Asset	Penyebab	Risiko	Dampak terhadap Bisnis
People	Staff	Catatan password/informasi sensitif disimpan di tempat yang dapat diakses publik	*Human error*	• Menurunnya reputasi • Proses bisnis terganggu
People	Staff	Karyawan kurang memahami prosedur penanganan server down	*Human error*	Proses bisnis yang berkaitan dengan server terkait tidak berjalan
People	Staff	Kesalahan Prosedur kerja	*Human error*	Proses bisnis terganggu
People	Staff	Loading area dilakukan di tempat terbuka	*Human error*	• Menurunnya reputasi • Proses bisnis terganggu

Penilaian risiko dengan menggunakan metode FMEA hanya dilakukan hingga tahap *severity* dan *occurrence* saja. Sedangkan untuk penilaian *detection* akan dilakukan saat pemeriksaan audit berlangsung. Beberapa contoh penilaian risiko dapat dilihat pada Tabel 5.6

Tabel 5. 6 Penilaian risiko dengan FMEA

ID	Kategori Asset	Nama Asset	Penyebab	Risk-ID	Risiko	Occ	Dampak Langsung	Dampak terhadap Bisnis	Sev
RR-01	Hard ware	Genset	Genset tidak berfungsi ketika tenaga listrik DSI UA mengalami pemadaman	R-03	*Power Failure*	3	Jaringan internet *down* dan aset TI yang dimiliki tidak berfungsi sementara	Proses bisnis yang bergantung pada koneksi internet terganggu, sehingga produktivitas menurun	6
RR-02	Hard ware	UPS	Kebakaran pada baterai UPS	R-02	Kebakaran	3	• Kehilangan data • Kerusakan pada aset TI yang dimiliki	Proses bisnis seluruhnya terhenti jika api tidak dapat dipadamkan	10

ID	Kategori Asset	Nama Asset	Penyebab	Risk-ID	Risiko	Occ	Dampak Langsung	Dampak terhadap Bisnis	Sev
							• Mengancam keselamatan staff		
RR-03	Hard ware	UPS	Kebakaran pada baterai UPS	R-02	Kebakaran	3	Jaringan internet down	Proses bisnis yang bergantung pada koneksi internet terganggu, sehingga produktivitas menurun	6
RR-04	Hard ware	UPS	Kegagalan fungsi UPS untuk menyuplai listrik karena kesalahan konfigurasi	R-03	*Power Failure*	3	Jaringan internet down dan aset TI yang dimiliki tidak berfungsi sementara	Proses bisnis yang bergantung pada koneksi internet terganggu, sehingga produktivitas menurun	6

Hasil penilaian 34 risiko dengan menggunakan metode FMEA secara lengkap dapat dilihat pada Lampiran C.

5.7. Pemetaan Risiko terhadap Kontrol ISO/IEC 27002:2013 Klausul Keamanan Fisik dan Lingkungan

Hasil dari analisis dan penilaian risiko akan dipetakan dalam control ISO/IEC 27002:2013 klausul kemanan fisik dan lingkungan. Pemetaan dilakukan dengan menghubungkan antara risiko dan penyebab yang ada dengan *implementation guide* kontrol yang ada pada klausul 11. Pemetaan terhadap *implementation guide* dan kontrol ini akan memastikan apakah organisasi telah menerapkan kontrol yang tepat untuk menangani risiko. Tabel 5.7 berikut ini adalah hasil pemetaan risiko terhadap control yang ada.

Tabel 5. 7 Pemetaan Risiko terhadap ISO 27002

ID	Ketegori Asset	Nama Asset	Penyebab	Risk -ID	Risiko	Pemetaan
RR -01	Hardware	Genset	Genset tidak berfungsi ketika tenaga listrik DSI UA mengalami pemadaman	R-03	*Power Failure*	*11.2.2 Supporting Utilities (implementation guide poin b dan c)*
RR -02	Hardware	UPS	Kebakaran pada baterai UPS	R-02	Kebakaran	*11.1.4 Protecting against external and environmental threats (seluruh implementation guide)* *11.2.2 Supporting Utilities (implementation guide poin c dan d)*
RR -03	Hardware	UPS	Kebakaran pada baterai UPS	R-02	Kebakaran	*11.1.4 Protecting against external and environmental threats (seluruh implementation guide)* *11.2.2 Supporting Utilities (implementation guide poin c dan d)*

ID	Ketegori Asset	Nama Asset	Penyebab	Risk -ID	Risiko	Pemetaan
RR -04	Hardware	UPS	Kegagalan fungsi UPS untuk menyuplai listrik karena kesalahan konfigurasi	R-03	*Power Failure*	*11.2.2 Supporting Utilities (implementation guide poin b dan c)*
RR -05	Hardware	Server	Petir, Angin kencang	R-01	Bencana Alam	*11.1.4 Protecting against external and environmental threats (seluruh implementation guide)*
RR -06	Hardware	Server	Gempa Bumi	R-01	Bencana Alam	*11.1.4 Protecting against external and environmental threats (seluruh implementation guide)*
RR -07	Hardware	Server	Kesalahan prosedur kerja saat melakukan perawatan fisik server	R-08	*Human error*	*11.2.4 Equipment maintenance (seluruh implementation guide)*
RR -08	Hardware	Server	*Improper Maintenance*	R-05	*Hardware Failure*	*11.2.4 Equipment maintenance (seluruh implementation guide)*

ID	Ketegori Asset	Nama Asset	Penyebab	Risk -ID	Risiko	Pemetaan
RR -09	Hardware	*Personal Computer* (PC)	Proses *maintenance* aset tidak dilakukan dengan benar	R-05	*Hardware Failure*	*11.2.4 Equipment maintenance (seluruh implementation guide)*
RR -10	Hardware	*Smoke Detector*	Proses *maintenance smoke detector* tidak dilakukan dengan benar	R-05	*Hardware Failure*	*11.2.4 Equipment maintenance (seluruh implementation guide)*
RR -11	Hardware	*Smoke Detector*	*Smoke detector* sudah usang	R-05	*Hardware Failure*	*11.2.4 Equipment maintenance (seluruh implementation guide)*
RR -12	Hardware	Pendingin ruangan	Proses monitoring suhu ruangan data center tidak dilakukan dengan maksimal	R-09	Pelanggaran regulasi	*11.2.1 Equipment siting and protection (implementation guide poin g)*
RR -13	Hardware	Perangkat Storage (Harddisk, Removable Media)	Kerusakan fisik	R-05	*Hardware Failure*	*11.2.1 Equipment siting and protection (implementation guide poin a, d, g, dan h)* *11.2.4 Equipment maintenance (seluruh implementation guide)*

ID	Ketegori Asset	Nama Asset	Penyebab	Risk -ID	Risiko	Pemetaan
RR -14	Hardware	Perangkat Storage (Harddisk, Removable Media)	Aktivitas pembuangan media penyimpanan tidak sesuai prosedur	R-09	Pelanggaran regulasi	*11.2.7 Secure disposal or re-use of equipment (seluruh implementation guide)* *11.2.5 Removal of property (implementation guide poin c)*
RR -15	Hardware	CCTV	Kesalahan pada tata letak CCTV	R-05	*Hardware Failure*	*11.2.1 Equipment siting and protection (implementation guide poin a, d, g, dan h)* *11.2.4 Equipment maintenance (seluruh implementation guide)*
RR -16	Hardware	Perangkat Penyimpanan dan penataan Server (rak, lemari, soket)	Kesalahan pengaturan tata letak dan keamanan di ruang server	R-07	Pencurian data fisik	*11.1.1 Physical security perimeter (implementation guide poin b, d, e, dan g)* *11.1.2 Physical entry controls (implementation guide poin c)* *11.1.3 Securing offices, rooms and*

ID	Ketegori Asset	Nama Asset	Penyebab	Risk -ID	Risiko	Pemetaan
						facilities (implementation guide poin a)
RR -17	Hardware	Perangkat Listrik	Terjadi konsleting/hubungan arus pendek	R-03	*Power Failure*	*11.2.3 Cabling security (implementation guide poin c.3)*
RR -18	Hardware	Perangkat Listrik	Terjadi konsleting/hubungan arus pendek	R-02	Kebakaran	*11.1.4 Protecting against external and environmental threats (seluruh implementation guide)* *11.2.3 Cabling security (implementation guide poin c.3)*
RR -19	Hardware	Perangkat Listrik	Gangguan panel listrik	R-03	*Power Failure*	*11.2.2 Supporting Utilities (implementation guide poin b dan c)*
RR -20	Hardware	Perangkat Listrik	Gangguan panel listrik	R-02	Kebakaran	*11.1.4 Protecting against external and environmental threats (seluruh implementation guide)*
RR -21	Hardware	Perangkat jaringan	Konfigurasi keamanan lemah	R-06	*Network Failure*	*11.2.1 Equipment siting and protection (implementation guide*

ID	Ketegori Asset	Nama Asset	Penyebab	Risk -ID	Risiko	Pemetaan
		(Switch, Router)				*poin c dan i)* *11.2.3 Cabling security (implementation guide poin a dan c.3)*
RR -22	Hardware	HUB	Kesalahan konfigurasi	R-05	*Hardware Failure*	*11.2.4 Equipment maintenance (seluruh implementation guide)*
RR -23	Hardware	Fingerprint	Sidik jari pegawai tidak terbaca	R-05	*Hardware Failure*	*11.2.1 Equipment siting and protection (implementation guide poin a, d, g, dan h)* *11.2.4 Equipment maintenance (seluruh implementation guide)*
RR -24	Hardware	Kabel Jaringan	Penempatan kabel jaringan yang tidak baik	R-06	*Network Failure*	*11.2.3 Cabling security (implementation guide poin a dan c.3)*
RR -25	Network	Jaringan MPLS	Kesalahan instalasi kabel	R-04	Pelanggaran SLA	*11.2.3 Cabling security (implementation guide poin a dan b)*

ID	Ketegori Asset	Nama Asset	Penyebab	Risk -ID	Risiko	Pemetaan
RR -26	Network	Koneksi Internet	Kehilangan akses remote data ke server	R-06	*Network Failure*	*11.2.6 Security of equipment off premises (implementation guide poin d)*
RR -27	People	Admin	Penyalahgunaan akses admin	R-09	Pelanggaran regulasi	*11.1.2 Physical entry controls (implementation guide poin c)*
RR -28	People	Staff	Pemberian hak akses yang tidak sesuai prosedur	R-09	Pelanggaran regulasi	*11.1.2 Physical entry controls (implementation guide poin c)*
RR -29	People	Staff	Kesalahan penggunaan akun	R-09	Pelanggaran regulasi	*11.1.2 Physical entry controls (implementation guide poin c)*
RR -30	People	Staff	PC ditinggalkan dalam keadaan *log-in* tanpa adanya penjagaan	R-08	*Human error*	*11.2.8 Unattended user equipment (implementation guide poin b)* *11.2.9 Clear desk and clear screen policy (implementation guide poin a)*
RR -31	People	Staff	Catatan password/informasi sensitif disimpan di	R-08	*Human error*	*11.2.9 Clear desk and clear screen policy (implementation guide poin a)*

ID	Ketegori Asset	Nama Asset	Penyebab	Risk -ID	Risiko	Pemetaan
			tempat yang dapat diakses publik			
RR -32	People	Staff	Karyawan kurang memahami prosedur penanganan server down	R-08	*Human error*	*11.2.4 Equipment maintenance (seluruh implementation guide)*
RR -33	People	Staff	Kesalahan Prosedur kerja	R-08	*Human error*	*11.1.5 Working in secure areas (implementation guide poin a dan c)*
RR -34	People	Staff	Loading area dilakukan di tempat terbuka	R-08	*Human error*	*11.1.1 Physical perimeter Security (implementation guide poin e, f, dan g)* *11.1.2 Physical entry controls (implementation guide poin c)* *11.1.6 Public access, delivery and loading area (implementation guide poin b dan c)*

5.8. Penyusunan Dokumen *Audit Program*

Dalam penyusunan dokumen *audit program* untuk Direktorat Sistem Informasi berdasarkan ISO/IEC 27002:2013 klausul 11, terdapat pengembangan dari dokumen perangkat audit sebelumnya milik Pandu Gilas Anarkhi [5] dan Yudhis Cahyo Eko [6].

5.8.1. Komposisi Dokumen

Komposisi dan struktur dokumen *audit program* yang dikembangkan meliputi sebagai berikut.

1. **Informasi Umum**
   Informasi umum dalam dokumen *audit program* ini bersifat pengetahuan umum mengenai audit yang akan dilakukan.Informasi umum memiliki komposisi sebagai berikut:
   a. Tujuan
      Berisi mengenai tujuan dari pembuatan dokumen *audit program*.
   b. Analisis Risiko
      Berisi analisis risiko yang telah dilakukan oleh penulis sebelumnya di ruang lingkup yang telah ditentukan yaitu ruang server.
   c. *Control Objective*
      Berisi mengenai kontrol yang ada pada ISO/IEC 27002:2013 klausul 11 Keamanan Fisik dan lingkungan yang berjumlah 15 kontrol.
   d. Acuan
      Berisi dokumen apa saja yang sekiranya dibutuhkan oleh Auditor dalam melaksanakan pemeriksaan audit.
   e. Proses Audit
      Berisi mengenai proses yang seharusnya dilewati oleh auditor namun hanya garis besarnya saja.

2. **Penilaian Risiko**
   Penilaian risiko berisi mengenai seluruh risiko yang telah dianalisis dan diurutkan berdasarkan kategori risiko oleh penulis. Tujuan dari adanya struktur penilaian risiko adalah agar Auditor dapat mengetahui kontrol mana saja yang perlu diprioritaskan terlebih dahulu.
3. **Perangkat Audit**
   Perangkat audit merupakan bagian inti dari dokumen *audit program* yang memberikan daftar kontrol yang harus diperiksa oleh Auditor.

5.8.2. Pembuatan Prosedur Audit

Pembuatan Prosedur Audit memiliki aturan penamaan dokumen dan memiliki komponen yang ada di dalamnya.

1. **Aturan Penamaan Dokumen**
   Aturan penamaan dokumen prosedur audit akan mempermudah dalam menggunakan dokumen. Komposisi penamaan dokumen prosedur audit adalah sebagai berikut:
   a. Nama Dokumen
      - P = Prosedur Audit
      - PTP = Pelaksanaan Tindak Lanjut Temuan
   b. Nomor Sub Klausul Kontrol yang berkaitan
   c. Nomor *control objective* dari sub klausul

   Sebagai contoh:
   Dokumen yang dibuat adalah prosedur audit yang mengambil kontrol 11.1.1 *Physical security perimeter*. Maka penamaan dokumen adalah:

   Dokumen prosedur audit memiliki kode **P**, dan kontrol tersebut dari sub klausul **1** dan kontrol objektif pertama, sehingga penamaannya adala **P.1.1**.

2. Struktur Dokumen

Prosedur audit berisi 15 dokumen yang telah disusun berdasarkan kontrol pada ISO/IEC 27002:2013 klausul 11 Keamanan Fisik dan Lingkungan. Tabel 5.8 berikut ini adalah 15 dokumen prosedur audit yang ada.

Tabel 5. 8 Daftar Prosedur Audit

No.	Id Dokumen	Nama Dokumen
1	P.1.1	Physical security perimeter
2	P.1.2	Physical entry controls
3	P.1.3	Securing offices, rooms and facilities
4	P.1.4	Protecting against external and environmental threats
5	P.1.5	Working in secure areas
6	P.1.6	Delivery and loading areas
7	P.2.1	Equipment siting and protection
8	P.2.2	Supporting utilities
9	P.2.3	Cabling security
10	P.2.4	Equipment maintenance
11	P.2.5	Removal of property
12	P.2.6	Security of equipment off premises
13	P.2.7	Secure disposal or re-use of equipment
14	P.2.8	Unattended User Equipment
15	P.2.9	Clear desk and clear screen policy

3. Komponen Dokumen

a. *Audit Checklist*

Setiap prosedur audit yang ada akan diuraikan lagi menjadi beberapa langkah pemeriksaan yang disebut *audit checklist*. *Audit checklist* berisi pertanyaan-pertanyaan yang dibagi menjadi pertanyaan *compliance* dan *substantive*. Jenis testing *compliance* menanyakan tentang ketersediaan sesuatu, sedangkan jenis *substantive* menanyakan kesesuaian suatu hal terhadap peraturan atau kebijakan yang ada.

Selain *audit checklist* dan jenis testing, prosedur audit berisi kolom *evidence* yang akan berisi bukti-bukti yang didapatkan auditor terkait dengan pertanyaan pada *audit checklist*. Kolom *evidence* akan diisikan oleh auditor saat pemeriksaan.

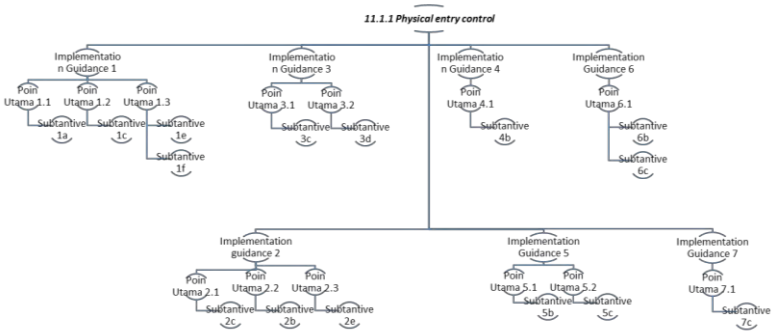
Salah satu contoh dari prosedur audit untuk *Control Objective* 11.1.1 *Physical security perimeter* dapat dilihat pada Gambar 5.3.

	PROSEDUR AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI RUANG SERVER UNIVERSITAS AIRLANGGA		
	11.1.1 Physical security perimeter	P.1.1	
	Kontrol: Perimeter keamanan (batasan seperti dinding, pintu masuk yang dikendalikan dengan kartu atau meja resepsionis yang dijaga) harus digunakan untuk melindungi area yang berisi informasi dan fasilitas pengolahan informasi.	AUDITOR	AUDITEE
PEMERIKSA :			
TANGGAL/JAM :			

Audit Procedure	*Testing*		*Audit Checklist*	*Yes*	*No*	*Partial*	*Evidence*
Auditor melakukan pengecekan terhadap perimeter keamanan yang digunakan untuk melindungi area yang berisi informasi penting: 1. Auditor mengumpulkan informasi mengenai peraturan perimeter keamanan yang digunakan di ruang server Universitas Airlangga	*Compliance*	a.	Tanyakan kepada kasi jaringan apakah terdapat perimeter keamanan informasi di ruang server? Jika ada mintakan dokumen daftar aset dari perimeter tersebut.				
	Substantive	a.	Apakah perimeter keamanan di ruang server telah sesuai dengan daftar aset perimeter keamanan yang dimiliki?				
	Compliance	c.	Adakah terdapat peraturan mengenai pengaturan dan penempatan perangkat keamanan di ruang server?				

Gambar 5. 3 Contoh Prosedur Audit

Setelah proses pemeriksaan dan pengisian satu prosedur audit, akan terdapat sebuah lembar hirarki audit prosedur yang telah diperiksa. Hirarki ini akan digunakan oleh auditor untuk mengetahui testing *substantive* mana sajakah yang belum memenuhi standar atau peraturan yang ada dengan cara memberi *shading* pada setiap poin *substantive*-nya. Gambar 5.4 berikut ini merupakan contoh hirarki prosedur audit untuk *Control Objective* 11.1.1 *Physical security perimeter*.



Gambar 5. 4 Contoh Hirarki Prosedur Audit

b. Formulir Laporan Pemeriksaan

Formulir laporan pemeriksaan dibuat untuk memudahkan auditor dalam merangkum temuan dari pemeriksaan sebuah kontrol yang telah dilakukan dan menuliskan saran perbaikan yang seharusnya dilakukan. Setiap elemen yang ada pada formulir laporan pemeriksaan didasarkan pada beberapa hal. Sesuai dengan ISO 19011 [13], proses audit harus jelas waktu dan objek pelaksanaan serta tim auditor yang melaksanakan proses audit. Maka dari itu, dalam laporan pemeriksaan ini diberikan kolom tanggal pemeriksaan, auditor dan auditee untuk memenuhi

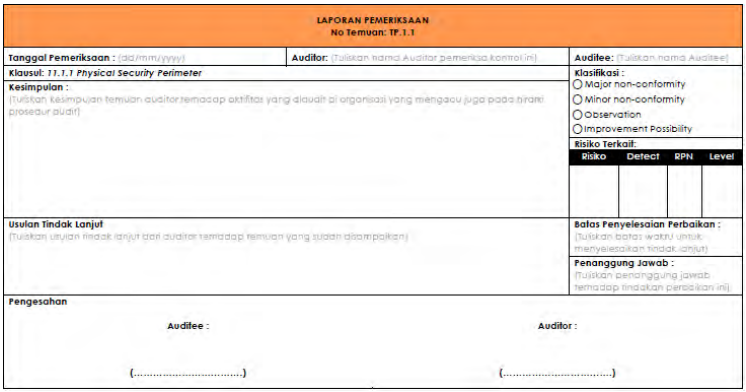
standar tersebut. Kolom "Tanggal Pemeriksaan" tersedia untuk menuliskan kapan audit terhadap sebuah kontrol yang tertulis pada kolom "Klausul" dilaksanakan. Kolom "Auditor" akan diisikan siapa yang bertugas melaksanakan audit pada kontrol yang tersedia, sedangkan kolom "Auditee" untuk diisi dengan unit atau orang-orang yang sedang diaudit. Selain itu, dalam proses audit ke 3 menurut ISO 19011 terdapat proses menghasilkan temuan audit. Temuan audit merupakan hal penting dalam proses audit, sehingga diberikan kolom "Kesimpulan" temuan dalam laporan pemeriksaan agar auditor lebih mudah menuliskan temuan-temuan yang telah didapatkan selama pada proses audit. Menurut Kagermann, et al [30] setiap temuan perlu diklasifikasikan utnuk menentukan prioritas dalam penyelesaian temuan yang ada. Pada laporan ini diberikan kolom "Klasifikasi" yang menyatakan seberapa penting temuan yang ada, dimana semakin tinggi tingkat klasifikasi maka tindak lanjut harus segera dilakukan. Pembagian klasifikasi menjadi 4 tingkat berdasarkan standar yang sudah biasa dipakai oleh pihak DSI Universitas Airlangga, yang penulis dapatkan melalui proses wawancara, dapat dilihat pada Lampiran A, tabel A.11.

Di lain hal, audit berbasis risiko bertujuan untuk memastikan risiko telah dikelola di dalam batasan risiko yang telah ditetapkan manajemen pada tingkatan korporasi [14], maka dari itu perlu adanya penilaian seberapa kontrol yang telah diterapkan organisasi untuk sebuah risiko yang ada. Hal ini disertakan dalam kolom "Risiko Terkait" yang berisi seberapa tinggi kontrol telah diterapkan dan level dari risiko, sehingga akan terlihat berapa level kepentingan sebuah risiko harus segera diselesaikan.

Dalam ISO 19011 proses keenam merupakan proses *audit follow-up* yang berisi tindak lanjut terhadap temuan yang ada. Penentuan tindak lanjut ini diberikan saat pemeriksaan audit selesai dilakukan, sehingga dalam laporan pemeriksaan juga diberikan kolom "Usulan Tindak Lanjut" akan berisikan saran perbaikan untuk mengatasi temuan yang ada sehingga risiko juga dapat teratasi. Saran perbaikan ini memiliki deadline kapan harus diselesaikan yang tercantum pada kolom "Batas Penyelesaian Perbaikan". Penentuan *deadline* perbaikan didapatkan dari klasifikasi temuan yang ada. Selain itu perbaikan dari temuan yang ada harus dilaksanakan sehingga perlu adanya penanggung jawab terhadap perbaikan. Maka kolom "Penanggung Jawab" disertakan untuk menuliskan siapa yang bertanggung jawab atas pelaksanaan perbaikan.

Kolom "Pengesahan" dicantumkan karena sesuai dengan proses audit yang ada menurut ISO 19011 bagian *planning* [13], di mana temuan yang didapatkan di setiap kontrol harus disetujui oleh kedua belah pihak, yaitu *auditee* dan *auditor*. Hal ini juga tercantum dalam jadwal di *audit plan* yaitu verifikasi temuan audit. Ketika pengesahan ini telah ditandatangani berarti pihak organisasi menerima apa yang telah dituliskan auditor dan akan melakukan perbaikan sesuai dengan batas waktu yang telah ditentukan.

Gambar 5.5 berikut ini merupakan contoh dari lembar kesimpulan temuan yang ada pada dokumen prosedur audit untuk C*ontrol Objective* 11.1.1 *Physical security perimeter*.



LAPORAN PEMERIKSAAN
No Temuan: TF.1.1

Tanggal Pemeriksaan : (dd/mm/yyyy)	**Auditor:** (Tuliskan nama Auditor pemeriksa kontrol ini)	**Auditee:** (Tuliskan nama Auditee)
Klausul: *11.1.1 Physical Security Perimeter*		**Klasifikasi :** ○ Major non-conformity ○ Minor non-conformity ○ Observation ○ Improvement Possibility
Kesimpulan : (Tuliskan kesimpulan temuan auditor terhadap aktifitas yang diaudit di organisasi yang mengacu juga pada hirarki prosedur audit)		**Risiko Terkait:** Risiko | Detect | RPN | Level
Usulan Tindak Lanjut (Tuliskan usulan tindak lanjut dari auditor terhadap temuan yang sudah disampaikan)		**Batas Penyelesaian Perbaikan :** (Tuliskan batas waktu untuk menyelesaikan tindak lanjut) **Penanggung Jawab :** (Tuliskan penanggung jawab terhadap tindakan perbaikan ini)
Pengesahan **Auditee :** (.....)		**Auditor :** (.....)

Gambar 5. 5 Contoh Kesimpulan Temuan Audit

5.8.3. Pembuatan Pelaksanaan Tindak lanjut

Tahap berikutnya setelah pembuatan prosedur audit adalah membuat pelaksaan tindak lanjut. Pelaksanaan tindak lanjut merupakan sebuah formulir yang berisikan tindak lanjut yang dilakukan oleh organisasi terkait dengan temuan audit yang telah dilakukan. Formulir ini akan diisikan oleh organisasi.

Kolom "Tanggal Audit" dicantumkan untuk mengetahui kapan audit terhadap kontrol yang ada pada kolom "Nama Kontrol" dilaksanakan. Kolom "Pelaksana" diisikan dengan siapa yang melaksanakan perbaikan, hal ini akan dicocokkan dengan Formulir Laporan Temuan apakah pelaksana sudah sesuai. Kolom "Pelaksanaan Tindak Lanjut" dicantumkan agar *Auditro* mengetahui apa tindakan yang dilakukan oleh organisasi terhadap temuan yang ada, sedangkan kolom "Tanggal Penyelesaian" akan memberikan informasi kepada auditor kapan tindak lanjut dilakukan, apakah sudah sesuai dengan *deadline* yang telah ditentukan sebelumnya. Kolom "Pengesahan" dicantumkan sebagai verifikasi antara pelaksana, auditor, dan direktur bahwa perbaikan telah dilakukan.

Gambar 5.6 menunjukkan formulir pelaksanaan tindak lanjut internal.

FORMULIR AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI RUANG SERVER UNIVERSITAS AIRLANGGA

PELAKSANAAN TINDAK LANJUT INTERNAL
No. Program: PTP.1.1.01

Tanggal Audit: (DD-MM-YYYY)

Nama Kontrol: (Isikan dengan nama control yang akan ditindaklanjuti)

Pelaksana : (Isikan nama pelaksana Tindak Lanjut)

Pelaksanaan Tindak Lanjut :
(Uraikan langkah Tindak Lanjut yang akan dilakukan oleh pelaksana)

Tanggal Penyelesaian: (DD-MM-YYYY)

Pengesahan

Pelaksana :	Lead Auditor :	Direktur Sistem Informasi:
(.....)	(.....)	(.....)

Gambar 5. 6 Formulir Pelaksaan Tindak Lanjut Audit

5.9. Penyusunan Dokumen Panduan Penggunaan Audit Program

Pada tahap ini, dokumen *audit program* yang ada akan dibuat panduan penggunaan *audit program* khususnya bagian prosedur audit. Panduan penggunaan ini berisi hal-hal sebagai berikut:

1. **Pendahuluan**
   Pada bagian ini merupakan bagian yang menjelaskan latar belakang pembuatan panduan penggunaan audit program. Dalam dokumen ini juga terdapat daftar audit prosedur yang telah dibuat.
2. **Panduan umum**
   Bagian ini menjelaskan mengenai petunjuk umum penggunaan dokumen audit program. Petunjuk ini digunakan untuk petunjuk pengisian maupun penggunaan dokumen yang dipakai hamper di seluruh dokumen audit program. Bagian panduan umum ini terdiri dari:
   a. Petunjuk Penggunaan Bagian Penilaian Risiko
   b. Petunjuk Pengisian Prosedur Audit
   c. Petunjuk Penggunaan Hirarki Prosedur Audit
   d. Petunjuk Pengisian Laporan Pemeriksaan
   e. Petunjuk Pengisian Tindak Lanjut Temuan Audit12
3. **Panduan Khusus**
   Panduan khusus merupakan panduan penggunaan yang bersifat khusus yang menjelaskan dokumen apa saja yang akan dibutuhkan oleh pihak auditor saat melaksanakan pemeriksaan.
4. **Pengecualian**
   Merupakan bagian yang menjelaskan pengecualian penggunaan dokumen ini. Dokumen panduan ini dibuat berdasarkan dokumen audit program yang telah dibuat penulis, sehingga jika akan mengubah dokumen maka organisasi harus menyesuaikan kembali dengan keadaan yang ada.

Gambar 5.7 berikut ini merupakan contoh dari isi panduan penggunaan audit.

GAMBAR 3 TATA URUTAN PENGISIAN PROSEDUR AUDIT

Dalam menggunakan prosedur audit, penting bagi auditor untuk memastikan bahwa perangkat yang digunakan adalah benar. Langkah yang dapat dilakukan adalah dengan memastikan bahawa ID dokumen telah benar dan sesuai dengan audit yang akan dilakukan.

Berikut merupakan tata urutan membaca dan menggunakan perangkat audit keamanan fisik dan lingkungan.

1. Langkah 1 Auditor harus benar-benar mebaca dan mengerti tujuan mengapa audit terhadap control objective ini dilakukan.
2. Langkah 2 Auditor memahami prosedur yang harus dijalankan dalam memulai suatu audit. Untuk setiap prosedur akan terdapat beberapa jenis testing dan audit checklist yang harus dilakukan oleh Auditor
3. Langkah 3 Auditor membaca, mengerti, dan memahami jenis testing yang akan Auditor lakukan pada setiap instruksi pemeriksaan audit yang nantinya akan dilakukan. Auditor harus benar-benar mengerti setiap Substantive dan Compliance testing yang harus dipenuhi.
4. Langkah 4 Auditor melakukan cek ketersediaan pendefinisian suatu objek dengan membaca, memahami, dan mengerti setiap checklist yang diajukan pada perangkat audit. Checklist harus diselesaikan semua bagian dengan melakukan pengisian daftar jawaban pada Langkah 6
5. Langkah 5 Auditor melakukan pengisian secara benar berdasarkan Audit Checklist dengan memberikan tanda **cek** (v) pada kolom yang sesuai. Dalam menjawab bagian ini, Auditor harus melakukan cek pada setiap Evidence dan Bukti Dokumen sesuai dengan Instruksi pemeriksaan yang diberikan.
6. Langkah 6 Auditor melakukan cek pada setiap dokumen atau keterangan yang tertera pada evidence untuk menentukan ketersediaan pendefinisian pada Audit Checklist.

Gambar 5. 7 Contoh Isi Panduan Penggunaan Audit Program

Halaman ini sengaja dikosongkan

BAB VI
HASIL DAN PEMBAHASAN

Bab ini akan menjelaskan hasil yang didapatkan dari penelitian ini, dan pembahasan secara keseluruhan yang didapatkan dari penelitian.

6.1. Verifikasi Dokumen Prosedur Audit

Pada poin ini dilakukan verifikasi terhadap prosedur audit yang telah dibuat. Tujuannya adalah untuk mengetahui kelengkapan dokumen prosedur audit yangtelah dibuat dengan kerangka ISO:IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan sebaga standar yang dijadikan acuan pada tugas akhir ini. Verifikasi dokumen prosedur audit dilakukan dengan cara *traceback* yaitu melakukan pengecekan kelengkapan prosedur audit yang ada dengan kontrol-kontrol yang ada pada ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan. Tabel verifikasi dokumen prosedur audit dapat dilihat pada Tabel 6.1 dibawah ini.

Tabel 6. 1 Verifikasi Dokumen Audit Prosedur P.1.1

Audit Prosedur		**ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan**			
#Pr	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
1	a, b	Pendefinisian perimeter keamanan	Perimeter keamanan harus didefinisikan, dan penentuan letak dan kekuatan dari masing-masing perimeter harus sesuai pada persyaratan keamanan aset dalam perimeter dan hasil penilaian risiko	*Physical security perimeter*	11.1.1
1	c, d	Penentuan letak dan kekuatan perimeter			
1	e, f, g	Penentuan perimeter keamanan dari risiko			

Audit Prosedur		**ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan**			
#Pr	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
2	a, b	Atap eksterior, dinding dan lantai area harus dari konstruksi yang solid	Perimeter bangunan atau situs yang berisi fasilitas pengolahan informasi harus *physically sound* (yaitu tidak boleh ada kesenjangan dalam perimeter atau daerah mana kerusakan bisa dengan mudah terjadi); atap eksterior, dinding dan lantai area harus dari konstruksi yang solid dan semua pintu eksternal harus sesuai dilindungi terhadap akses yang tidak sah dengan mekanisme kontrol, (misalnya bar, alarm, kunci); pintu dan jendela harus terkunci		
2	c	Perimeter bangunan harus *physically sound*			
2	d, e	Pelindungan pintu dari akses yang tidak sah			
3	a, c	Penyediaan meja resepsionis	Meja resepsionis yang dijaga atau hal lain untuk mengontrol akses fisik ke area atau bangunan harus		
3	b, d	Pembatasan akses ke area			

Audit Prosedur		ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan			
#*Pr*	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
			disediakan; akses ke area dan bangunan harus dibatasi untuk petugas yang berwenang saja		
4	a, b	Pembuatan pelindung fisik	Pelindung fisik, jika memungkinkan, harus dibangun untuk mencegah akses fisik tidak sah dan pencemaran lingkungan		
5	a, b	Pembuatan alarm untuk kebakaran	Semua pintu harus diberi alarm, dipantau dan diuji dalam hubungannya dengan dinding untuk menetapkan tingkat yang diperlukan terhadap perlawanan api sesuai dengan standar regional, nasional dan internasional yang sesuai		
5	c, d	Dinding yang kuat terhadap kebakaran			
6	a, b, c	Pemasangan system pendeteksi yang cocok	Sistem pendeteksi penyusup yang cocok harus dipasang dan secara teratur		

Audit Prosedur		ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan			
#*Pr*	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
			diuji yang mencakup pintu dan jendela yang mungkin diakses; daerah kosong harus diamankan		
7	a, b, c	Pemisahan fasilitas pengolahan informasi	Fasilitas pengolahan informasi yang dikelola oleh organisasi harus secara fisik dipisahkan dari yang dikelola oleh pihak eksternal		

Keterangan:

- Kolom **"#Pr"** pada kolom Audit Procedure menunjukkan nomor prosedur yang ada pada dokumen Audit Program bagian Perangkat Audit (kolom pertama pada tabel Prosedur Audit).
- Kolom **"#Audit checklist"** pada kolom Audit Procedure menunjukkan nomor checklist yang ada pada dokumen Audit Program bagian Perangkat Audit (kolom ketiga pada tabel Prosedur Audit).
- Kolom **"poin utama"** menunjukkan poin yang ada pada audit checklist dan hubungannya dengan ISO/IEC 27002:2013.
- Kolom **"implementation guide"** diambil dari ISO/IEC 27002:2013 yang dihubungkan dengan poin utama yang ada pada kolom sebelumnya.

- Kolom **"control objective"** diambil merupakan nama dari kendali tujuan (*control objective*) yang berkaitan dengan *implementation guide* yang ada.
- Kolom **"No. Kontrol"** menunjukkan dimana (nomor) *control objective* ada pada ISO/IEC 27002:2013.

Tabel verifikasi prosedur audit selengkapnya dapat dilihat pada bagian Lampiran C. Dari hasil verifikasi yang telah dilakukan dapat dilihat bahwa seluruh kontrol dan *implementation* guide dalam ISO/IEC 27002:2013 telah tercantum dalam seluruh dokumen prosedur audit yang ada.

6.2. Contoh Pengisian Dokumen Prosedur Audit

Contoh pengisian dokumen prosedur audit yang ada pada bagian Audit Program dapat dilihat pada Tabel 6.2.

Tabel 6. 2 Contoh Pengisian Prosedur Audit

	PROSEDUR AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI RUANG SERVER UNIVERSITAS AIRLANGGA		
	11.2.8 Unattended User Equipment	**P.2.8**	
	Kontrol: Peralatan yang ditinggalkan oleh penggunanya (unattended) harus dipastikan terlindungi dengan tepat	**AUDITOR MALIKHAH**	**AUDITEE ANDRY**
PEMERIKSA : Stephen Christian			
TANGGAL/JAM : 10 Desember 2014			

Audit Procedure	***Testing***	***Audit Checklist***	***Yes***	***No***	***Partial***	***Evidence***
Auditor melakukan pengecekan pada perangkat TI yang digunakan oleh staff saat ditinggalkan: 1.Auditor melakukan pengumpulan informasi mengenai perlindungan terhadap perangkat yang ditinggalkan	*Compliance*	a. Apakah tersedia dokumen prosedur kerja mengenai penggunaan peralatan TI di ruang server DSI Universitas Airlangga?	v			Dokumen prosedur kerja penggunaan peralatan di ruang server, seperti PC, printer, dan lain-lain tersedia. (Dokumen prosedur kerja akan dilampirkan)

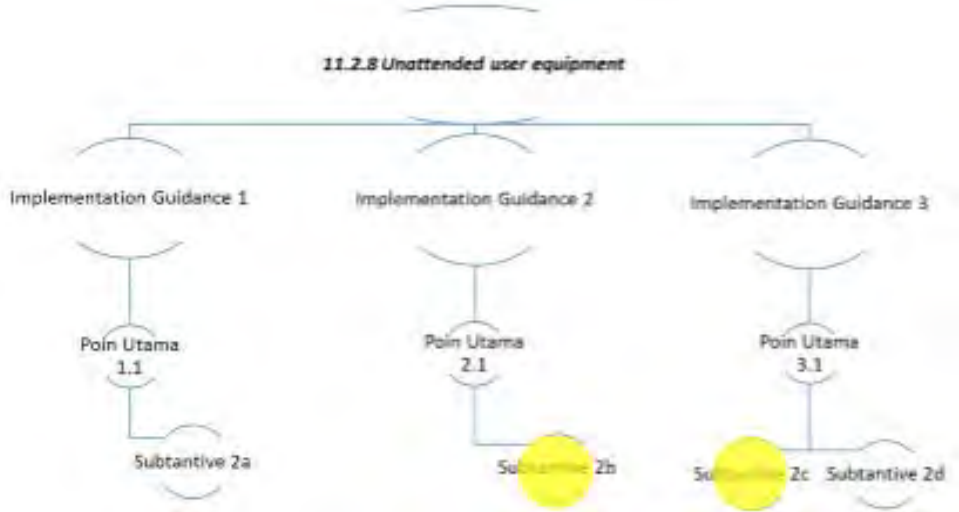
Audit Procedure	*Testing*	*Audit Checklist*	*Yes*	*No*	*Partial*	*Evidence*
		(Mintakan dokumen prosedur kerja tersebut)				
	Substantive	b. Apakah dokumen tersebut dimiliki dan dimengerti oleh seluruh staff yang berada di ruang server DSI Universitas Airlangga?	v			Staff yang berada di ruang server ada 4 orang, dan seluruh staff memahami peraturan yang ada. (Pencapaian 100%)
2. Auditor melakukan pengujian terkait dengan keamanan peralatan TI yang ditinggalkan (unattended)	*Substantive*	a. Apakah staff selalu terminating session setiap selesai menggunakan aplikasi? (Periksa di setiap komputer staff di ruang server, misal PHP dengan menggunakan kode session_destroy();)	v			Setiap staff di ruang server Universitas Airlangga selalu menutup aplikasi, hal ini terbukti dari pemeriksaan session yang ada (akan dilampirkan). (Pencapaian 100%)

Audit Procedure	*Testing*	*Audit Checklist*	*Yes*	*No*	*Partial*	*Evidence*
	Substantive	b. Apakah setiap kali perangkat TI (komputer) ditinggalkan selalu di log off? (Periksa di setiap komputer staff di ruang server dengan menggunakan Control Panel --> Administrative Tools --> Event Viewer)			v	Hanya ada 2 dari 4 orang yang tidak melakukan log off computer saat ditinggalkan dalam jangka waktu singkat. Hal ini terlihat dalam Event Viewer pada 2 terdapat jangka waktu *idle* yang cukup lama. (Pencapaian 50%)
	Substantive	c. Apakah peralatan TI staff, seperti PC dan handphone, dilengkapi dengan password?			v	Dari 4 komputer dan 6 handphone yang ada, hanya 3 komputer dan 3 handphone saja yang dilengkapi dengan password. (Pencapaian 62%)

Audit Procedure	*Testing*	*Audit Checklist*	*Yes*	*No*	*Partial*	*Evidence*
	Substantive	d. Apakah peralatan TI staff dilengkapi dengan fitur autolock dalam jangka waktu yang telah ditentukan sesuai prosedur?	v			Seluruh peralatan TI yang dimiliki oleh staff memiliki fitur autolock dalam jangka waktu antara 5-10 menit keadaan *idle*

Hirariki Prosedur Audit

P.2.8



LAPORAN PEMERIKSAAN
No Temuan: TP.2.8

Tanggal Pemeriksaan : 10/12/2015	**Auditor:** Malikhah	**Auditee:** Andry
Klausul: ***11.2.8 Unattended user equipment***		**Klasifikasi :** ◯ Major non-conformity ⊗ Minor non-conformity ◯ Observation ◯ Improvement Possibility
Kesimpulan : Secara umum, implementasi kontrol *Unattended User Equipment* telah dijalankan dengan cukup baik. Peraturan telah ada, namun beberapa masih belum dijalankan dengan baik oleh seluruh staff yang ada. Hal ini diperkuat dengan masih adanya staff yang tidak melakukan *log-off* saat computer ditinggalkan		**Risiko Terkait:** Risiko: **RR-30** · Detect: **4** · RPN: **100** · Level: **Medium**
Usulan Tindak Lanjut Perlu adanya sosialisasi lebih lanjut agar seluruh staff memahami pentingnya mematuhi peraturan yang ada. Selain itu perlu adanya pengawasan dari pihak kepala seksi dalam penerapan kontrol ini. Dapat juga memberikan peringatan sampai dengan sanksi kepada staff yang melanggar.		**Batas Penyelesaian Perbaikan :** 10/06/2016 (6 bulan) **Penanggung Jawab :** Andry

6.3. Persetujuan Panduan Audit

Pada bagian ini dijelaskan mengenai proses validasi luaran penelitian yaitu dokumen panduan audit yang berisi dokumen *audit plan* dan *audit program*.

6.3.1. Perencanaan Proses Persetujuan

Persetujuan akan dilakukan dengan menggunakan metode *acceptance testing* kepada pihak Direktorat Sistem Informasi Universitas Airlangga, khususnya pada bagian Keamanan Data, karena bagian ini mengetahui proses audit yang biasanya dilakukandi lingkungan Direktorat Sistem Informasi. *Acceptance Testing* akan dilakukan melalui email dan tatap muka. Perencanaan aktivitas persetujuan dapat dilihat pada Tabel 6.3

Tabel 6. 3 Perencanaan Persetujuan Panduan Audit

Jenis Validasi	Validasi Dokumen melalui email	
Pelaku	Kepala Seksi (Kasi) Keamanan Data	
Aktivitas	**No.**	**Deskripsi**
	1.	Peneliti mengirimkan dokumen *audit plan audit program* kepada Kasi Keamanan Data untuk di-*review*.
	2.	Peneliti menerima beberapa masukan dari Kasi Keamanan Data mengenai informasi jadwal yang ada di dalam *Audit Plan*.
	3.	Peneliti melakukan perbaikan pada dokumen *Audit Plan*.
	4.	Peneliti kembali mengirimkan hasil *Audit Plan* yang telah diperbaiki kepada Kasi Keamanan Data.

	6.	Kasi Keamanan Data menyetujui perubahan terakhir.
	7.	Peneliti memberikan hasil *audit program* yang telah disusun.
	8.	Kasi Keamanan Data memberikan masukan terkait dengan template temuan pemeriksaan.
	9.	Peneliti memperbaiki dokumen *Audit Program* sesuai dengan masukan yang telah diterima sebelumnya.
	10.	Peneliti mengirimkan hasil perbaikan *Audit Program* kepada pihak DSI melalui Kasi Keamanan Data.
	11.	Kasi Keamanan Data menyetujui perubahan terakhir.
	12.	Peneliti merekap masukan yang diterima dan mendokumentasikannya.

6.3.2. Hasil Persetujuan Panduan Audit

Hasil dari persetujuan yang didapatkan melalui masukan dari Kasi Keamanan Data ditunjukkan dengan perubahan di beberapa bagian dokumen seperti dijelaskan di bawah ini.

1. Pendefinisian Auditor dan Auditee untuk Audit Internal Direktorat Sistem Informasi Universitas Airlangga.
   - Perubahan ini terjadi pada dokumen *Audit Plan* pada Informasi umum.
   - Gambar 6.1 Dan 6.2 berikut ini merupakan perubahan yang telah dilakukan pada bagian informasi umum:

1.6 Kontak

Untuk mendapatkan informasi lebih lanjut dalam pelaksanaan kegiatan audit mengenai keamanan fisik dan lingkungan teknologi informasi di ruang server Direktorat Sistem Informasi Universitas Airlangga maka dapat menghubungi ke kontak dibawah ini:

1.6.1 Auditor (SPI)

Nama	:	
Email	:	
Nama	:	
Email	:	
Nama	:	
Email	:	

1.6.2 Auditee

Nama	:	
Jabatan	:	Kasi Jaringan
Email	:	
Nama	:	
Jabatan	:	Staff Jaringan
Email	:	
Nama	:	
Jabatan	:	Staff Jaringan
Email	:	

Gambar 6. 1 Kontak Audit Sebelum Perbaikan

1.6 Kontak

Untuk mendapatkan informasi lebih lanjut dalam pelaksanaan kegiatan audit mengenai keamanan fisik dan lingkungan teknologi informasi di ruang server Direktorat Sistem Informasi Universitas Airlangga maka dapat menghubungi ke kontak dibawah ini:

1.6.1 Auditor (SPI)

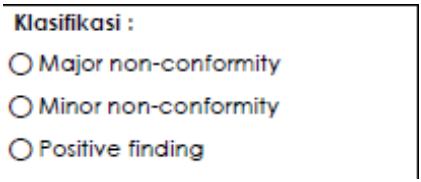
Nama	:	Indri Sulistyowati
Email	:	indri@staff.unair.ac.id
Nama	:	Malikhah
Email	:	malikhah@staff.unair.ac.id
Nama	:	Musa
Email	:	musa@staff.unair.ac.id

1.6.2 Auditee

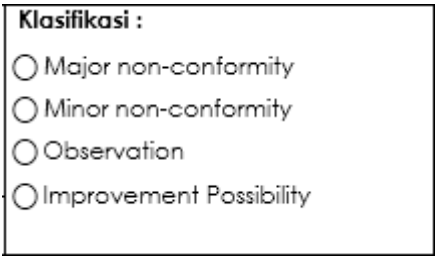
Nama	:	Andri Tamtrijanto
Jabatan	:	Kepala Seksi Jaringan
Email	:	andri@staff.unair.ac.id
Nama	:	Dedy Priyambodo
Jabatan	:	Staff Sekssi Jaringan
Email	:	dedy@staff.unair.ac.id
Nama	:	Andry Yudianto
Jabatan	:	Staff Sekssi Jaringan
Email	:	andry@staff.unair.ac.id
Nama	:	Indrayana
Jabatan	:	Staff Sekssi Jaringan
Email	:	indrayana@staff.unair.ac.id

Gambar 6. 2 Kontak Audit Setelah Perbaikan

2. Durasi pelaksaan proses pemeriksaan audit internal.
   - Perbaikan audit ini berada pada dokumen *Audit Plan* pada bagian jadwal kegiatan. Perbaikan dilakukan dengan mengurangi waktu audit untuk mendekati keadaan sebenarnya di DSI.
   - Rincian sebelum perubahan adalah sebagai berikut:
     - Initiation : Dari 4 hari menjadi 2 hari
     - Planning : Dari 4 hari menjadi 18 hari
     - Execution : Dari 5 hari menjadi 2.75 hari
     - Closing : Dari 7 hari menjadi 0.5 hari
3. Klasifikasi temuan yang ada pada formulir temuan pemeriksaan.
   - Perbaikan audit ini berada pada dokumen *Audit rogram* pada bagian formulir temuan pemeriksaan. Perbaikan dilakukan dengan menyesuaikan klasifikasi yang biasa digunakan oleh pihak DSI. Gambar 6.3 dan Gambar 6.4 memberikan visualisasi mengenai perubahan yang dilakukan.

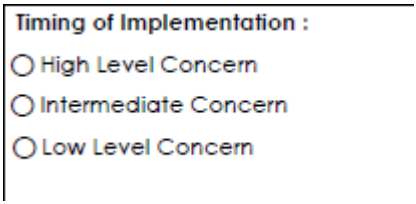


Gambar 6. 3 Klasifikasi Temuan Sebelum Perubahan



Gambar 6. 4 Klasifikasi Temuan Setelah Perubahan

4. Waktu pelaksanaan pada formulir temuan pemeriksaan.
    - Perbaikan audit ini berada pada dokumen *Audit rogram* pada bagian formulir temuan pemeriksaan. Perbaikan dilakukan dengan menghapus pilhan waktu perbaikan dengan yang biasa digunakan oleh DSI. Gambar 6.5 dan Gambar 6.5 memberikan visualisasi mengenai perubahan yang dilakukan.



Gambar 6. 5 Waktu Perbaikan Sebelum Perubahan

Gambar 6. 6 Waktu Perbaikan Setelah Perubahan

Hasil wawancara untuk proses pengesahan dokumen dapat dilihat pada ampiran A Tabel A.10 dan Tabel A.11. Sedangkan untuk persetujuan dapat dilihat pada Lampiran E.

BAB VII
KESIMPULAN DAN SARAN

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

7.1. Kesimpulan

Berdasarkan proses dan tahapan yang telah dilakukan dalam pengerjaan tugas akhir ini, maka dapat diambil kesimpulan-kesimpulan yang menjawab rumusan masalah yang telah ditentukan, yaitu:

1. Dalam dokumen *Audit Plan* terdapat jadwal audit yang terdiri dari 4 aktivitas yaitu *Initiation*, *Planning, Execution,* dan *Closing*. Aktivitas yang membutuhkan banyak interaksi dengan *auditee* adalah bagian *Execution*.
2. Berdasarkan hasil identifikasi risiko yang telah dilakukan, didapatkan sembilan kategori risiko. Dari delapan kategori risiko tersebut dilakukan analisis untuk mengetahui *potential risk* yang dapat muncul dari setiap kategori. Hasilnya didapatkan sebanyak 34 *risk register* yang termasuk dalam kontrol keamanan fisik dan lingkungan.
3. Dari hasil pemetaan risiko ,maka didapatkan bahwa seluruh kontrol dalam ISO 27002:2013 klausul 11 Keamanan Fisik dan Lingkungan digunakan seluruhnya dalam pemetaan risiko. Namun penggunaan *implementation guide* seluruhnya hanya pada 5 kontrol saja, yaitu kontrol 11.1.4, 11.2.3, 11.2.4, dan 11.2.7.
4. Dalam perangkat audit terdapat prosedur audit yang berisi 15 *control objective* audit untuk melakukan pemeriksaan *compliance* dan *substantive* yang mengacu pada ISO/IEC 27002:2013 klausul 11 dengan total 59 prosedur, 95 testing *compliance* dan 101 testing *substantive*. Semakin banyak prosedur pada suatu *control objective* maka semakin banyak testing *compliance* dan *substantive* nya.

7.2. Saran

Saran yang dapat penulis sampaikan untuk penelitian selanjutnya adalah sebagai berikut:

1. Pemetaan risiko dalam kontrol yang terdapat pada ISO/IEC 27002:2013 pada penelitian ini menggunakan identifikasi risiko yang dibuat oleh penulis. Pemetaan risiko juga dapat menggunakan identifikasi risiko yang dilakukan oleh organisasi.
2. Pada proses pembuatan prosedur audit, penelitian selanjutnya dapat lebih mendetailkan *implementation guidance* yang terdapat pada setiap kontrol, sehingga pembuatan prosedur audit lebih baik dan rinci.

DAFTAR PUSTAKA

[1] K. I. Anasthasia, “Teknologi Informasi Dalam Organisasi,” Jimbaran, 2011.

[2] B. Raharjo, “Pemanfaatan Teknologi Informasi di Perguruan Tinggi "Sosialisasi Mengenai Implementasi Penerapan UU No. 19 Tahun 2002 Tentang Hak Cipta; Pemerintah Sebagai Panutan Dalam Ketaatan Lisensi Peranti Lunak",” Bandung, 2004.

[3] M. Kamat, ISO 27001 Security Guideline for Information Asset Valuation, 2009.

[4] M. A. Ramadhan, Pembuatan Perangkat Audit Internal TI berbasis Resiko menggunakan ISO/IEC 27002:2007 pada Proses Pengelolaan Data Studi Kasus Digital Library ITS, Surabaya: ITS, 2011.

[5] P. G. Anarkhi, Penyusunan Perangkat Audit Kemanan Informasi Aplikasi Berbasis Web menggunakan ISO/IEC 27001 Klausul Kendali Akses, Surabaya: ITS, 2012.

[6] Y. E. Cahyo, Pembuatan Panduan Audit Teknologi Informasi pada Proses Pengelolaan Lingkungan Fisik berbasis COBIT 5 di KPPN Surabaya II, Surabaya: ITS, 2014.

[7] A. Arens and J. K. Loebbecke, Auditing and Assurance Services, 7th Edition, New Jersey: Prentice Hall, 1997.

[8] S. Agoes, Auditing (Pemeriksaan Akuntan), Edisi 2, Jakarta: Fakultas Ekonomi Universitas Indonesia, 1996.

[9] R. Weber, Information System Controls and Audit, Upper Saddle River, New Jersey: Prentice Hall, 2000.

[10] L. P. Willcocks, Investing in information systems: evaluation and management, London, UK: Chapman and Hall, 1995.

[11] National E-Governance Plan, Information Security Management in e-governance, India: Department of Electronics and Information Technology, 2014.

[12] G. Popescu, V. A. Popescu and C. R. Popescu, Information Systems Security Audit, Bucharest: Gestiuena Publishing House, 2006.

[13] ISO, ISO 19011: Guidelines for auditing management, Switzerland: ISO, 2011.

[14] T. M. Tuanakotta, Audit Berbasis ISA, Jakarta: Salemba Empat, 2013.

[15] H. R. Satriadi, Perancangan Buku Panduan Survival di Hutan Tropis, Bandung: Universitas Widyatama, 2010.

[16] Austin Community College, "Audit a Class," 03 Nopember 2009. [Online]. Available: http://www.austincc.edu/audit/documents/AuditCharter091103.pdf.

[17] G. Stoneburner, "Risk Management Guide for Information Technology Systems," 2002.

[18] M. Spremic, Emerging issues in IT Governance: Implementing the Corporate IT Risk Management Model, 2008.

[19] C. Gygi and B. Williams, Six Sigma For Dummies, 2nd Edition, Hoboken: John Wiley & Sons, Inc., 2012.

[20] Dyadem Press, Guidelines for Failure Mode and Effects Analysis for Automotive, Aerospace, and General Manufacturing Industries, Richmond Hill: CRC Press, 2003.

[21] “Control Objective ISO 27001.pdf”.

[22] A. G. Woodside, Case Study Research: Theory, Methods, Practice, Bingley: Emerald Group Publishing Limited, 2010.

[23] C. B. Meyer, “A Case Study Methodology,” p. 330, 17 May 2011.

[24] R. K. Yin, Case Study Research Design and Method, Sage Publication, 1994.

[25] S. A. Baboucarr Njie, “Case Study as a Choice in Qualitative Methodology,” *IOSR Journal of Research & Method in Education (IOSR-JRME),* vol. 4, no. 3, pp. 35-40, 2014.

[26] J. C. McKinney, Constrctive Typology and Social Theory, New York: Aplleton-Century-Crofts, 1966.

[27] R. Yin, Case Study Research Design and Method, Newbury Park: Sage, 1989.

[28] R. Yin, Case study research: Design and methods (3rd ed.), Thousand Oaks: CA: Sage, 2003.

[29] S. Hudri, “Jenis dan Teknik atau Metode,” 2013. [Online]. Available: http://expresisastra.blogspot.com. [Accessed 28 March 2015].

Halaman ini sengaja dikosongkan

LAMPIRAN A.
HASIL WAWANCARA

Pada poin Lampiran A ini akan diberikan daftar wawancara yang sudah dilakukan oleh penulis ke pihak Direktorat Sistem Informasi universitas Airlangga.

Tabel A. 1 Wawancara Pengajuan Tugas Akhir

Tanggal Wawancara	**:** 6 Maret 2015
Via	**:** SMS
Jabatan Narasumber	**:** Kepala Seksi Keamanan Data
Tujuan Wawancara	**:** Pengajuan Tugas Akhir

Pertanyaan	Jawaban
Selamat pagi Mbak Indri, saya Stephen mahasiswa SI ITS yang semester kemarin KP di DSI. Kali ini saya mau mengajukan Tugas Akhir dengan objek DSI apakah boleh?	Boleh, silahkan saja. Topik apa yang kamu ambil? Apa melanjutkan dari yang kemarin?
Iya Mbak, saya ambil topic Audit Keamanan Informasi.	*Basic*nya apa? ISO atau COBIT?
ISO 27002	Oke, yang terbaru ya, yang 2013 karena kita sudah adopsi yang terbaru.
Oh harus yang 2013 ya mbak? Oke kalau begitu	Jangan lupa surat pengantarnya jurusan ya. Serahkan ke DSI terus kita ketemu setelah kamu lulus siding proposal aja.
Baik mbak, terimakasih banyak.	Ok.

Tabel A. 2 Wawancara Kondisi Kekinian Organisasi

Tanggal Wawancara	: 24 April 2014
Via	: Tatap muka
Jabatan Narasumber	: Kepala Seksi Keamanan Data
Tujuan Wawancara	: Kondisi organisasi

Pertanyaan	Jawaban
Selamat pagi Mbak Indri, saya sudah selesai siding proposal dan sudah disetujui.	*Yawes,* kamu pake ISO 27000 yang 2013 kan? Sudah ada *handout* nya?
Kalau yang 27002 sudah ada mbak, tapi yang ISO 27001 belum ada. Tapi saya sepertinya hanya butuh yang ISO 27002.	Oke. Kamu mau audit apanya di DSI sini? Kan banyak, toh ga mungkin semuanya kamu audit kan.
Iya mbak, Cuma 1 bagian aja, yang keamanan fisik dan lingkungan.	Lho, kok ambil yang itu? Kenapa ga kontrol akses atau pengelolaan aset aja yang lebih TI?
Iya mbak, maaf sebelumnya kalau tidak begitu ke TI, tapi menurut saya bagian ini penting karena bagian ini menjadi penjamin keamanan proses bisnis yang dilakukan di DSI sini.	Yasudah, gak masalah. Tapi mungkin saya ga bisa bantu banyak kalo dalam hal itu. Kan itu ngomongin soal gedung-gedung sama tembok kaya gitu kan?
Tidak Cuma itu mbak, tapi ada pengamanan untuk IT nya sendiri, kebijakan-kebijkan penggunaan IT itu juga. Pasti DSI kan punya pengaturan sendiri.	Iya ada beberapa kok.
Mbak, seperti waktu kerja praktik kemarin kan DSI ada struktur organisasi, apakah setiap subdit punya tupoksi masing-masing?	Seksi maksudmu? Kalo setiap seksi ada. Nanti saya kirim kalau kamu butuh. Tulis terus kasih aku alamat emailmu ya
Oh iya mbak seksi maksud saya. Baik mbak, terimakasih. Nah lingkup ruang kerjanya staff DSI itu ada berapa sih mbak?	Lingkup ruang kerja ya di sini. Ini bagian utama, kerja kita semua di sini.
Oh, terus kalau yang ruang helpdesk dipojok sana yang tempat saya KP itu bukan punya DSI?	Oh yang itu juga punya DSI, kalau ada urusan seperti mengurus cybercampus unair

Pertanyaan	Jawaban
	kemaren mahasiswa datang ke tempat itu.
Terus kalau tidak salah di dalam ada seperti ruang server gitu ya mbak, kok ada tulisannya *restricted area*?	Iya itu data center kita. Gak semua orang bias masuk ke sana. Makanya kemarin waktu kalian KP cuman bisa di ruang helpdesk
begitu ya mbak, jadi data centernya itu data center Unair? DSI juga yang mengurus?	Iyalah.
Dari ruang pusat ini, helpdesk, sama data center mana yang paling penting mbak?	Ya penting semua. Kalo ga ada salah satu proses bisnis kita timpang dong. Jadi Semua penting.
Iya mbak, tapi kalau misalkan terjadi kerusakan, cuma misal sih, itu yang mana yang paling berpengaruh terhadap proses bisnis?	Ya jangan sampai, makanya kita ada kontrol-kontrol keamanan.Tapi paling berpengaruh ya tempat kerja pusat sama data center. Kalau ruang helpdesk kan ya gitu-gitu aja, ga ada IT yang ada di sana. Tapi karena helpdesk nyambung sama ruang data center ya jadi penting juga.
imact kalau terjadi kerusakan itu yang paling kerasa yang mana?	Ya itu tadi semua kerasa, kalo di ruang kerja ini kan data-data pegawai yang dikerjakan buat Unair ini, kalau yang di data center itu data satu unair bener-bener disimpan di sana. Jadi kalau sampai data center rusak ya sudah, datanya Unair hilang, proses bisnis yang bergantung sama intrnet lumpuh.
Begitu ya mbak. Kalau data center siapa yang bertanggung jawab di sana?	Kalau di data center yang bertanggung jawab seksi jaringan.

Pertanyaan	Jawaban
Jaringan bertugas seluruhnya di sana?	Iya, ruang data center tempat kerjanya seksi jaringan. Mereka yang bertanggung jawab sama semua yang ada di sana.
Berapa orang mbak yang ada di sana?	Ya semua orang staffnya jaringan. Sebentar. Ada 4 orang kalau tidak salah.
Mbak kalau saya ambil data center untuk objek bagaimana?	Ya tidak masalah.

Tabel A. 3 Wawancara Kegiatan Audit di DSI UA

Tanggal Wawancara : 24 April 2014
Via : Tatap muka
Jabatan Narasumber : Kepala Seksi Keamanan Data
Tujuan Wawancara : Audit di DSI

Pertanyaan	Jawaban
Terima kasih buat izinnya mbak. Kalau untuk masalah audit, di sini dilakukan tiap apa mbak?	Jangka waktunya? Ya satu tahun sekali lah, itu sudah pakem dan minimalnya.
Jadi setiap tahun pasti diadakan audit ya?	Iya.
Itu setiap bulan apa mbak? Terjadwalkah?	Biasanya saat menjelang tutup buku. Kira-kira bulan Desember.
Berapa lama waktu auditnya?	Ya 2 hari biasanya.
Loh mbak cuman 2 hari? Kok cuman sebentar?	Kalau orangnya 2 ya 2 hari kerja, kan bebannya ada 4, jadi masing-masing 2. Tapi kalau orangnya 4 orang ya 1 hari selesai kan satu satu.

Pertanyaan	Jawaban
Auditornya cuman 2 orang mbak? Apa waktu segitu tidak terlalu cepat?	Jarang sih biasanya ya 4 orang turun semua. Efektif kok, ngapain lama-lama. Kan membuang biaya nanti jadinya. Toh prosesnya juga cuman sebentar.
Jadi diadakan Desember dan cuma 1-2 hari mbak? Kalau dibuat jadwal kira-kira tanggal berapa?	Iya, tapi gak tentu tanggalnya.Tulis aja Desember, soalnya biasanya bulan itu. Bareng sama evaluasi.
Baik mbak. Kalau evaluasi berarti ada juga mbak?	Ada.
Itu kapan mbak diadakannya?	Biasanya sih hamper bareng sama audit.
Orangnya yang ikut siapa?	Itu bentuknya rapat besar, jadi seluruh staff dikumpulkan buat evaluasi. Mulai dari finansia;l sampai keamanan TI.
Jadi audit sama evaluasi ada semua dan diadakan di hari yang sama ya mbak?	Harinya tidak barengan, ya mana bisa, tapi ya hamper berdekatan lah waktunya.
Kembali lagi ke audit mbak, kalau dihubungkan dengan focus topic saya, siapa yang terlibat?	Kalau di ruang server ya staff jaringan.
Jadi kasi dengan staff menjadi objek audit ya mbak? Apa hanya itu?	Ya kalau soal keamanan fisik kan kita ga ngatur semuanya, ada sebagian besar yang siatur sama bagian sumber daya, seperti pengelolaan lokasi, removal peralatan kan yang ngatur sumber daya. Kalau seperti itu ya kita akan panggil juga mereka untuk di audit.
Wah jadi lintas direktorat ya mbak?	Iya. Karena DSi kan ga mungkin ngerjakan semua sendirian, DSI juga masih di

Pertanyaan	Jawaban
	bawah naungan Unair, jadi harus ikut peraturan sama strukturnya Unair.

Tabel A. 4 Wawancara Penerapan ISO 27002 kalusul 11 di DSI

Tanggal Wawancara : 24 April 2014
Via : Tatap muka
Jabatan Narasumber : Kepala Seksi Keamanan Data
Tujuan Wawancara : Penerapan ISO 27002 klausul 11

Pertanyaan	Jawaban
Untuk kontrol yang saya ambil, apakah diterapkan semua?	Aku sampai lupa kamu ambil yang mana tadi?
Keamanan Fisik dan Lingkungan mbak	Oh iya, ya harus diterapkan semua. ISO 27000 itu satu paket satu kesatuan gak boleh yang ini dipakai, yang ini gak dipakai. Jadi harus semuanya.
Jadi seluruh kontrol kan di sini ada 6 sama 9 kontrol, jadinya 15 itu diterapkan semua?	Iya seperti yang saya bilang itu sebuah kesatuan. Tapia da kalanya sebuah organisasi tidak bisa menerapkan itu karena mereka tidak punya itu atau tidak punya hak untuk mengatur itu. Contohnya kalo di DSI kita ga bisa milih karyawan yang bisa masuk, kan dipilihkan dari Unair. Tapi dilain hal kita bisa mengatur buat sesuai sama kontrl ISO yang lainnya.
Sebagian besar 17 konrol diterapkan berarti ya mbak sama unair?	Iya, tapi kan ISO itu nda saklek juga peraturannya harus seperti ini itu, kaya loading area ini, kita kan ga punya sendiri-sendiri, jadi satu ya di depan. Kalo di ISO kan harus tertutup,

	diberi keamanan dan segala macem.
Iya mbak, kalau begitu terima kasih infonya yang banyak ini, maaf mengganggu waktunya.	Sudah? Cuman segini aja? Saya kira banyak yang mau ditanyakan. Ya sudah. Selamat mengerjakan TA ya, cepat lulus.

Tabel A. 5 Wawancara Aset TI di ruang server

Tanggal Wawancara : 30 April 2014
Via : Email
Jabatan Narasumber : Kepala Seksi Keamanan Data
Tujuan Wawancara : Aset

Pertanyaan	Jawaban
Selamat siang mbak. Mohon maaf apa saya boleh minta data terkait tentang: 1. Aset TI di ruang server? 2. Tupoksi yang kemarin belum dikirm Terima kasih sebelumnya.	

Tabel A. 6 Wawancara Aset TI di ruang server (2)

Tanggal Wawancara : 2 Mei 2014
Via : SMS
Jabatan Narasumber : Kepala Seksi Keamanan Data
Tujuan Wawancara : Aset TI di ruang server

Pertanyaan	Jawaban
Selamat siang mbak. Mohon maaf kemarin saya sudah kirim email menanyakan tupoksi dan aset TI. Mohon responnya.	Maaf ya, saya sedang sibuk, coba cek email.

	Oh iya kalau untuk identifikasi risiko coba kamu dulu yang buat.

Tabel A. 7 Wawancara Aset TI di ruang server (3)

Tanggal Wawancara : 2 Mei 2014
Via : SMS
Jabatan Narasumber : Kepala Seksi Keamanan Data
Tujuan Wawancara : Aset TI di ruang server

Pertanyaan	Jawaban
	Untuk aset yang ada didata center saya tdk bisa memberikan, untuk gambaran umumnya: 1. Aset Hardware : server, router, catalist, firewall, UPS, AC, CCTV 2. Aset software : OS, VM , database, bandwidth manajemen, firewall, software monitoring network dan log Silahkan tambahkan sendiri seperti yang kamu tahu waktu KP.
Oh baik mbak, aset itu saja sudah cukup, saya akan tambahkan sendiri. terima kasih banyak dan maaf mengganggu	Ok.

Tabel A. 8 Verifikasi Penilaian Risiko

Tanggal Wawancara : 20 Mei 2014
Via : Skype
Jabatan Narasumber : Kepala Seksi Keamanan Data
Tujuan Wawancara : Risk Assessment

Pertanyaan	Jawaban
Selamat sore mbak, maaf mengganggu via telepon di jam kerja. Bagaimana review dokumen risikonya?	Iya, sudah saya baca, tapi saya masih belum terbiasa dengan metode yang kamu pakai. Ini bentuknya penilaian gitu ya? Apa sama yang seperti kamu KP?
Iya mbak, itu sama seperti KP, pakai FMEA.	Identifikasi risikomu sudah cukup banyak. Tapi saya masih bingung dengan Risk sama risk register yang kamu maksud disini.
Kalau risk nya itu risiko secara umum mbak, jadi saya kelompok-kelompokkan. Kalau risk register itu yang secara detailnya, jadi *hardware* failure pasti banyak penyebabnya ya itu yang saya jabarkan.	Hmm, gimana kalau dihapus saja yg R ini. Tapi ga usah juga gapapa sih, saya sudah mulai paham. Ini kamu analisisnya dapat dari mana?
Saya dapat dari kemungkinan risiko TI yang mungkin terjadi. Kan kalau risiko TI sepertinya ya itu-itu saja yang terjadi.	Iya benar. Ini sudah cukup umum terjadi. Ini kamu mencantumkan yang sudah pernah terjadi kira-kira?
Iya mbak.	Seharusnya ada penilaian untuk yang belum pernah terjadi atau untuk masa depan jadi kita bisa siap-siap.
Oh begitu ya mbak, tapi kalau dilakukan penilaian kan jadi tidak bisa soalnya DSI belum pernah mengalami.	Iya sih, kamu pakai penilaian probabilitas juga ya, yasudah ini saja cukup. Tapi coba

Pertanyaan	Jawaban
	dipikirkan lagi mungkin ada yang kurang.
Baik mbak, apakah ada lagi? Untuk deteksi sama nilai-nilainya bagaimana?	Mitigasi sudah cukup benar sih, mungkin ada beberapa perubahan yang perlu. Untuk yang penilaiannya saya pelajari dulu ya referansi penilaian mu.
Iya mbak, jadi untuk mitigasi apa mbak yang mengganti atau seperti apa?	Iya saya saja yang ganti daripada ribet. Untuk penilaian kalau saya sudah selesai memahami metodenya, dan kalau ada yang salah saya akan coba ubah.
Baik mbak, saya akan coba cari risiko lainnya, kalau ada saya akan hubungi lagi. Terima kasih banyak, maaf juga sudah merepotkan sampai seperti ini.	Iya tidak apa.

Tabel A. 9 Verifikasi Penilaian Risiko (2)

Tanggal Wawancara : 1 Juni 2014
Via : SMS
Jabatan Narasumber : Kepala Seksi Keamanan Data
Tujuan Wawancara : Risk Assessment

Pertanyaan	Jawaban
Selamat pagi mbak. Bagaimana dengan risk assessment saya?	Maaf ya, saya sedang cukup sibuk ini. Saya akan coba selesaikan hari ini atau besok.

Tabel A. 10 Verifikasi dokumen Audit Plan

Tanggal Wawancara : 13 Mei 2014
Via : Skype
Jabatan Narasumber : Kepala Seksi Keamanan Data
Tujuan Wawancara : Verifikasi Informasi *Audit plan*

Pertanyaan	Jawaban
Selamat pagi mbak. Bagaimana dengan dokumen *audit plan* yang saya buat?	Ini yang harus saya periksa yang mana? Semuanya?
Tidak perlu mbak, hanya untuk bagian yang pertama, informasi umum saja. Terutama yang informasi auditor dan auditee.	Oh. Untuk informasi umum sudah oke, scope nya data center ya? Ini audite-nya staff bagian jaringan saja semuanya. Kamu masukkan informasi alamat email saja ya.
Oh baik mbak. Untuk auditor-nya bagaimana?	Auditornya 4 orang. Bagian keamanan data bertugas untuk jadi auditor. Ada saya, malikhah sama 2 orang lainnya. Kamu lihat sendiri saja.
Baik. Ini untuk jadwal audit saya sudah buatkan 4 hari pemeriksaan sesuai dengan yang dilakukan di sini.	Cukup ribet ya, kita di sini tidak menggunakan proses seperti ini. Kita ada acuan sendiri, tapi kita tidak bisa memberi tahu.
Begitu ya mbak, soalnya saya menyusun jadwal ini berdasarkan ISO 19011.	Ya sudah kalau itu acuan kamu, mungkin memang sedikit berbeda.
Jadi bagaimana?	Kalau kita di sini sih tidak samapi 1 minggu. Jadi untuk proses audit kita memang 4 hari, tergantung apa yang diperiksa, dan untuk bagian *closing* tidak sampai 2 hari kok. Tapi kalau ini memang acuan kamu dan berbeda dengan proses kita tidak apa juga. Kan pasti kamu

Pertanyaan	Jawaban
	juga punya pertimbangan sendiri
Iya mbak, nanti saya akan coba perbaiki lagi untuk bagian jadwalnya.	Oke
Baik kalau begitu, terima kasih untuk informasi dan waktunya.	Iya sama-sama.

Tabel A. 11 Verifikasi Dokumen Audit Program

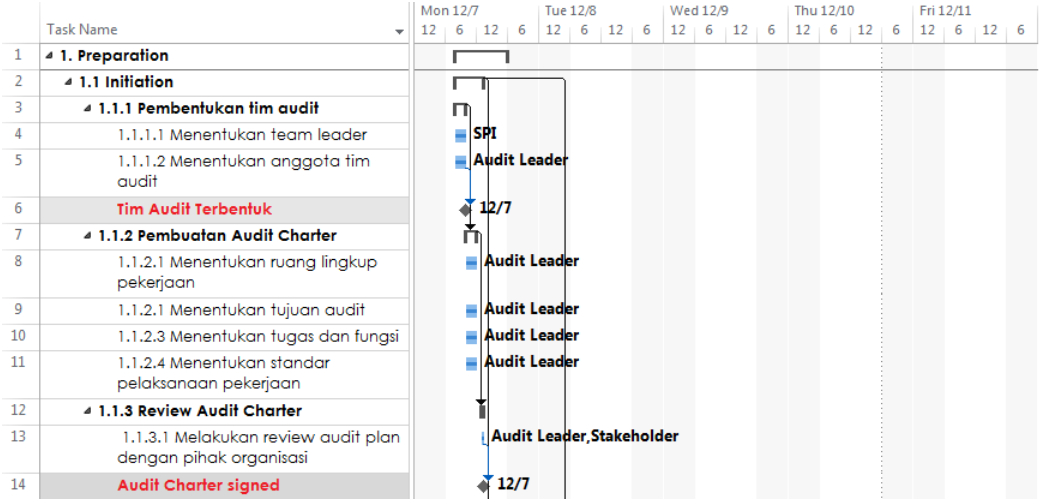
Tanggal Wawancara : 15 Juni 2014
Via : Tatap Muka
Jabatan Narasumber : Kepala Seksi Keamanan Data
Tujuan Wawancara : Verifikasi *Audit Program*

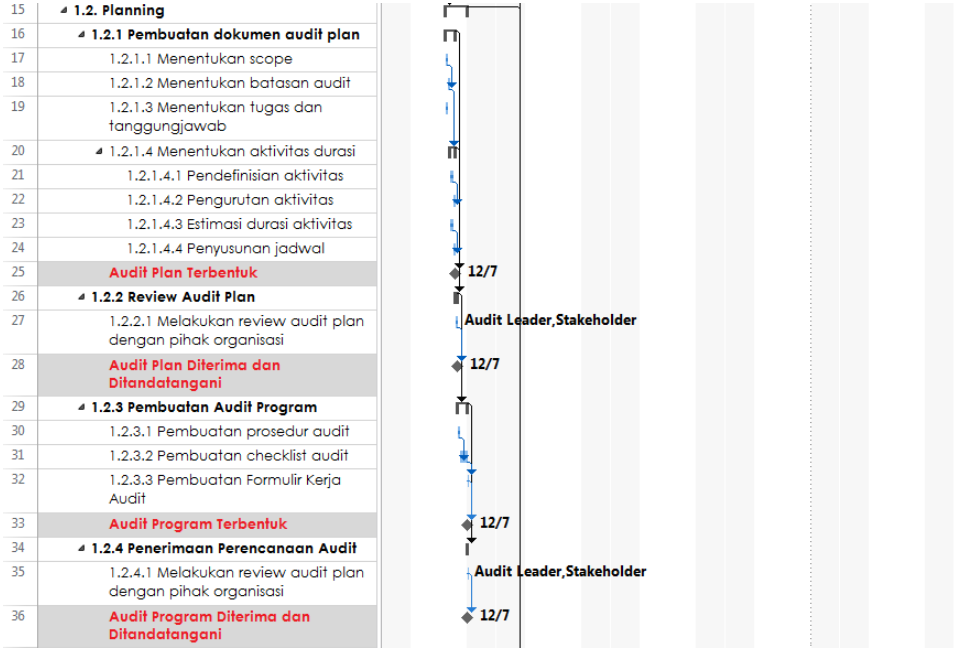
Pertanyaan	Jawaban
Selamat pagi mbak. Ini dokumen *audit program* yang sudah saya buat.	Tebel banget ya. Bentar ya saya cek dulu.
Iya mbak, solanya itu per kontrol di klausul 11 saya masukkan di sana.	Ini ceklistnya ya, ya seperti ini saja sudah oke.
Untuk temuan auditnya bagaimana?	Ini ya temuan auditnya? Klasifikasinya jadi 4 kalau di sini, mayor, minor, observasi sama improvement. Yang paling kecil improvement. Coba kamu nanti cari di ISO 17000 sekian.
Jadi 4 ya mbak, iya nanti saya perbaiki lagi.	Untuk pelaksanaan ini *piye* maksudnya?
Ya kan ada temuan terus ada tindakan perbaikan pasti, nah itu auditor menentukan mana konsentrasinya yang harus didulukan.	Ga perlu pakai kaya gitu, mending nanti ditulis aja. Kalo mayor berarti maksimal 2 bulan, minor 6 bulan dan seterusnya gitu.

Noted mbak, nanti saya ubah juga.	Itu saja sih, *overall* sudah cukup.
Untuk bagian formulir pelaksanaan tindak lanjut bagaimana?	Apalagi ini?
Ya kalau auditee selesai melakukan perbaikan nanti dicatatnya di sini.	Oalah, kita ga pakai beginian. Kan kita TI, mikirnya ribet, yasudah nanti auditornya yang mengecek setelah batas waktu selesai. Tapi kalaupun dipakai juga gak masalah sih.
Baik mbak nanti formulir temuan yang saya benarkan. Naksih banyak mbak.	Oke. Semangat ya.

LAMPIRAN B.
JADWAL AKTIVITAS AUDIT

Pada bagian ini diberikan contoh isi dari *Audit Plan*. Bagian *Audit Plan* yang akan diberikan adalah bagian *Gantt chart* yang mencakup seluruh aktivitas audit beserta jadwalnya.




15 1.2. Planning
16 1.2.1 Pembuatan dokumen audit plan
17 1.2.1.1 Menentukan scope
18 1.2.1.2 Menentukan batasan audit
19 1.2.1.3 Menentukan tugas dan tanggungjawab
20 1.2.1.4 Menentukan aktivitas durasi
21 1.2.1.4.1 Pendefinisian aktivitas
22 1.2.1.4.2 Pengurutan aktivitas
23 1.2.1.4.3 Estimasi durasi aktivitas
24 1.2.1.4.4 Penyusunan jadwal
25 Audit Plan Terbentuk
26 1.2.2 Review Audit Plan
27 1.2.2.1 Melakukan review audit plan dengan pihak organisasi
28 Audit Plan Diterima dan Ditandatangani
29 1.2.3 Pembuatan Audit Program
30 1.2.3.1 Pembuatan prosedur audit
31 1.2.3.2 Pembuatan checklist audit
32 1.2.3.3 Pembuatan Formulir Kerja Audit
33 Audit Program Terbentuk
34 1.2.4 Penerimaan Perencanaan Audit
35 1.2.4.1 Melakukan review audit plan dengan pihak organisasi
36 Audit Program Diterima dan Ditandatangani
12/7
Audit Leader,Stakeholder
12/7
12/7
Audit Leader,Stakeholder
12/7

37	**2. Execution**	Auditor 1,Auditor 2,Auditor 3
38	**2.1 Opening Meeting**	Auditor 1,Auditor 2,Auditor 3
39	**2.2 Melakukan pengujian audit**	Auditor 1,Auditor 2,Auditor 3
40	2.2.1 Melakukan uji compliance	Audit Leader
41	2.2.2 Melakukan uji substantif	12/9
42	2.2.3 Melakukan judging materiality	Audit Leader,Stakeholder
43	2.2.4 Melakukan evaluasi audit risk	12/9
44	**Temuan ketidaksesuaian proses terhadap kontrol**	
45	2.3 Verifikasi temuan audit	Auditor 1,Auditor 2,Auditor 3
46	**Persetujuan kedua belah pihak terkait temuan**	Audit Leader
47	**2.4 Mendokumentasikan kegiatan audit**	12/10
48	2.4.1 Melengkapi audit checklist	Audit Leader
49	2.4.2 Menyiapkan simpulan audit	Audit Leader
50	**Proses audit terdokumentasi**	Audit Leader
51	**2.5 Closing meeting**	12/10
52	2.5.1 Review Implementasi audit	
53	2.5.2 Rekomendasi auditor	
54	2.5.3 Pemaparan penilaian audit	
55	**Closing meeting telah selesai dilakukan**	
56	**3. Closing**	Auditor 1
57	3.1 Menyusun draft laporan audit	Audit Leader,Stakeholder
58	3.2 Mengkomunikasian draft laporan dengan pihak auditee	12/10
59	**Persetujuan kedua belah pihak terkait hasil audit**	Auditor 2
60	3.3 Menyusun laporan akhir	Audit Leader,Auditor 1
61	3.4 Mengkomunikasikan laporan akhir audit kepada auditee	,Auditor 2,Auditor 3,Stakeholder
62	**Laporan akhir audit disetujui dan diserah**	12/10

LAMPIRAN C.
HASIL PENILAIAN RISIKO DENGAN METODE FMEA

Halaman ini sengaja dikosongkan

Lampiran C ini akan memberikan daftar risiko beserta penilaiannya dengan menggunakan metode FMEA.

Tabel C. 1 Hasil Penilaian Risiko Aset TI DSI UA dengan Metode FMEA

ID	Kategori Asset	Nama Asset	Penyebab	Risk-ID	Risiko	Occ	Dampak Langsung	Dampak terhadap Bisnis	Sev
RR-01	Hardware	Genset	Genset tidak berfungsi ketika tenaga listrik DSI UA mengalami pemadaman	R-03	*Power Failure*	3	Jaringan internet *down*dan kerusakan pada aset TI yang dimiliki	Proses bisnis yang bergantung pada koneksi internet terganggu, sehingga produktivitas menurun	6
RR-02	Hardware	UPS	Kebakaran pada baterai UPS	R-02	Kebakaran	3	• Kehilangan data • Kerusakan pada aset TI yang dimiliki	Proses bisnis seluruhnya terhenti jika tidak dapat dipadamkan	10

ID	Kategori Asset	Nama Asset	Penyebab	Risk-ID	Risiko	Occ	Dampak Langsung	Dampak terhadap Bisnis	Sev
							• Mengancam keselamatan staff		
RR-03	Hardware	UPS	Kebakaran pada baterai UPS	R-02	Kebakaran	3	Jaringan internet down dan kerusakan pada aset TI yang dimiliki	Proses bisnis yang bergantung pada koneksi internet terganggu, sehingga produktivitas menurun	6
RR-04	Hardware	UPS	Kegagalan fungsi UPS untuk menyuplai listrik	R-03	*Power Failure*	3	Jaringan internet down dan kerusakan	Proses bisnis yang bergantung pada koneksi internet	6

ID	Kategori Asset	Nama Asset	Penyebab	Risk-ID	Risiko	Occ	Dampak Langsung	Dampak terhadap Bisnis	Sev
			karena kesalahan konfigurasi				pada aset TI yang dimiliki	terganggu, sehingga produktivitas menurun	
RR-05	Hardware	Server	Petir, Angin kencang	R-01	Bencana Alam	3	Kerusakan aset TI, Kehilangan data	Proses bisnis yang berkaitan dengan server yang rusak terhenti hingga server dapat pulih	6
RR-06	Hardware	Server	Gempa Bumi	R-01	Bencana Alam	1	• Bangunan Runtuh • Kerusakan pada aset TI yang dimiliki • Mengancam	Proses bisnis terhenti	10

ID	Kategori Asset	Nama Asset	Penyebab	Risk-ID	Risiko	Occ	Dampak Langsung	Dampak terhadap Bisnis	Sev
							keselamatan staff		
RR-07	Hardware	Server	Kesalahan prosedur kerja saat melakukan perawatan fisik server	R-08	*Human error*	4	• Kerusakan pada aset TI yang dimiliki • Mengancam keselamatan staff • Kehilangan data	Proses bisnis yang berkaitan dengan server yang rusak terhenti hingga server dapat pulih	10
RR-08	Hardware	Server	*Improper Maintenance*	R-05	*Hardware Failure*	3	• Kerusakan pada aset TI yang dimiliki	Proses bisnis yang berkaitan dengan server yang rusak	5

ID	Kategori Asset	Nama Asset	Penyebab	Risk-ID	Risiko	Occ	Dampak Langsung	Dampak terhadap Bisnis	Sev
							• Kehilangan data	terhenti hingga server dapat pulih	
RR-09	Hardware	*Personal Computer* (PC)	Proses *maintenance* aset tidak dilakukan dengan benar	R-05	*Hardware Failure*	4	Kerusakan PC	Proses bisnis yang berkaitan dengan PC tersebut terganggu, sehingga produktivitas menurun	4
RR-10	Hardware	*Smoke Detector*	Proses *maintenance smoke detector* tidak dilakukan dengan benar	R-05	*Hardware Failure*	4	• Kerusakan pada aset TI yang dimiliki • Kebakaran • Mengancam keselamatan	Proses bisnis seluruhnya terhenti jika tidak dapat dipadamkan	10

ID	Kategori Asset	Nama Asset	Penyebab	Risk-ID	Risiko	Occ	Dampak Langsung	Dampak terhadap Bisnis	Sev
							staff • Kehilangan data		
RR-11	Hardware	*Smoke Detector*	*Smoke detector* sudah usang	R-05	*Hardware Failure*	2	• Kerusakan pada aset TI yang dimiliki • Kebakaran • Mengancam keselamatan staff • Kehilangan data	Proses bisnis seluruhnya terhenti jika tidak dapat dipadamkan	10

ID	Kategori Asset	Nama Asset	Penyebab	Risk-ID	Risiko	Occ	Dampak Langsung	Dampak terhadap Bisnis	Sev
RR-12	Hardware	Pendingin ruangan	Proses monitoring suhu ruangan data center tidak dilakukan dengan maksimal	R-09	Pelanggaran regulasi	2	Suhu server terlalu panas sehingga menyebabkan kebakaran	Proses bisnis yang berkaitan dengan server yang rusak terhenti hingga server dapat pulih	8
RR-13	Hardware	Perangkat Storage (Harddisk, Removable Media)	Kerusakan fisik	R-05	*Hardware Failure*	2	Data hilang	Sebagian proses bisnis yang terkait dengan data yang rusak terganggu, sehingga produktivitas menurun	9
RR-14	Hardware	Perangkat Storage (Harddisk,	Aktivitas pembuangan media	R-09	Pelanggaran regulasi	3	*Data recovery* oleh pihak	Menurunnya reputasi	7

ID	Kategori Asset	Nama Asset	Penyebab	Risk-ID	Risiko	Occ	Dampak Langsung	Dampak terhadap Bisnis	Sev
		Removable Media)	penyimpanan tidak sesuai prosedur				yang tidak berwenang		
RR-15	Hardware	CCTV	Kesalahan pada tata letak CCTV	R-05	*Hardware Failure*	3	Blind spot dimanfaatkan oleh pihak tak bertanggung jawab untuk melakukan hal yang merugikan DSI UA (Pencurian)	• Menurunnya reputasi • Proses bisnis terganggu	6

ID	Kategori Asset	Nama Asset	Penyebab	Risk-ID	Risiko	Occ	Dampak Langsung	Dampak terhadap Bisnis	Sev
RR-16	Hardware	Perangkat Penyimpanan dan penataan Server (rak, lemari, soket)	Kesalahan pengaturan tata letak dan keamanan di ruang server	R-07	Pencurian data fisik	3	• Manipulasi data • Kebocoran informasi •Data hilang	• Menurunnya reputasi • Proses bisnis terganggu	6
RR-17	Hardware	Perangkat Listrik	Terjadi konsleting/hubungan arus pendek	R-03	*Power Failure*	3	Jaringan internet *down*dan kerusakan pada aset TI yang dimiliki	Proses bisnis yang bergantung pada koneksi internet terganggu, sehingga produktivitas menurun	6

ID	Kategori Asset	Nama Asset	Penyebab	Risk-ID	Risiko	Occ	Dampak Langsung	Dampak terhadap Bisnis	Sev
RR-18	Hardware	Perangkat Listrik	Terjadi konsleting/hubungan arus pendek	R-02	Kebakaran	3	Mengancam keselamatan staff	Proses bisnis akan terhenti	10
RR-19	Hardware	Perangkat Listrik	Gangguan panel listrik	R-03	*Power Failure*	3	Jaringan internet *down*dan kerusakan pada aset TI yang dimiliki	Proses bisnis yang bergantung pada koneksi internet terganggu, sehingga produktivitas menurun	6
RR-20	Hardware	Perangkat Listrik	Gangguan panel listrik	R-02	Kebakaran	3	Mengancam keselamatan staff	Proses bisnis akan terhenti	10

ID	Kategori Asset	Nama Asset	Penyebab	Risk-ID	Risiko	Occ	Dampak Langsung	Dampak terhadap Bisnis	Sev
RR-21	Hardware	Perangkat jaringan (Switch, Router)	Konfigurasi keamanan lemah	R-06	*Network Failure*	2	• Manipulasi data • Kebocoran informasi •Data hilang • IP Spoofing	• Menurunnya reputasi • Proses bisnis terganggu	6
RR-22	Hardware	HUB	Kesalahan konfigurasi	R-05	*Hardware Failure*	3	Perangkat jaringan komputer tidak terhubung	Proses bisnis terganggu	7

ID	Kategori Asset	Nama Asset	Penyebab	Risk-ID	Risiko	Occ	Dampak Langsung	Dampak terhadap Bisnis	Sev
RR-23	Hardware	Fingerprint	Sidik jari pegawai tidak terbaca	R-05	*Hardware Failure*	5	• Kebocoran informasi • Pencatatan karyawan yang masuk ruang server terganggu	• Menurunnya reputasi • Proses bisnis terganggu	6
RR-24	Hardware	Kabel Jaringan	Penempatan kabel jaringan yang tidak baik	R-06	*Network Failure*	4	Jaringan internet *down*	Proses bisnis yang bergantung pada koneksi internet terganggu, sehingga produktivitas menurun	6

ID	Kategori Asset	Nama Asset	Penyebab	Risk-ID	Risiko	Occ	Dampak Langsung	Dampak terhadap Bisnis	Sev
RR-25	Network	Jaringan MPLS	Kurang monitoring dan review SLA	R-04	Pelanggaran SLA	5	layanan internet down dan availability menurun	Proses bisnis yang bergantung pada koneksi internet terganggu, sehingga produktivitas menurun	6
RR-26	Network	Koneksi Internet	Kehilangan akses remote data ke server	R-06	*Network Failure*	3	• Aplikasi tidak berjalan sebagaimana mestinya (*crash*) • Data hilang	• Proses bisnis yang berkaitan dengan aplikasi tersebut terganggu • Menurunnya reputasi	7

ID	Kategori Asset	Nama Asset	Penyebab	Risk-ID	Risiko	Occ	Dampak Langsung	Dampak terhadap Bisnis	Sev
RR-27	People	Admin	Penyalahgunaan akses admin	R-09	Pelanggaran regulasi	5	• hilangnya kontrol dari admin • Manipulasi data • Kebocoran informasi • Data hilang	• Menurunnya reputasi • Proses bisnis terganggu	6
RR-28	People	Staff	Pemberian hak akses yang tidak sesuai prosedur	R-09	Pelanggaran regulasi	3	• Manipulasi data • Kebocoran informasi • Data hilang	• Menurunnya reputasi • Proses bisnis terganggu	5

ID	Kategori Asset	Nama Asset	Penyebab	Risk-ID	Risiko	Occ	Dampak Langsung	Dampak terhadap Bisnis	Sev
RR-29	People	Staff	Kesalahan penggunaan akun	R-09	Pelanggaran regulasi	4	Akun tidak bisa digunakan	Proses bisnis terhambat	4
RR-30	People	Staff	PC ditinggalkan dalam keadaan *log-in* tanpa adanya penjagaan	R-08	*Human error*	5	• Manipulasi data • Kebocoran informasi • Data hilang	• Menurunnya reputasi • Proses bisnis terganggu	5
RR-31	People	Staff	Catatan password/informasi sensitif disimpan di tempat yang dapat diakses publik	R-08	*Human error*	5	• Manipulasi data • Kebocoran informasi • Data hilang	• Menurunnya reputasi • Proses bisnis terganggu	5

ID	Kategori Asset	Nama Asset	Penyebab	Risk-ID	Risiko	Occ	Dampak Langsung	Dampak terhadap Bisnis	Sev
RR-32	People	Staff	Karyawan kurang memahami prosedur penanganan server down	R-08	*Human error*	3	Kerusakan pada aset TI yang dimiliki	Proses bisnis yang berkaitan dengan server terkait tidak berjalan	5
RR-33	People	Staff	Kesalahan Prosedur kerja	R-08	*Human error*	3	• Kerusakan pada aset TI yang dimiliki • Keselamatan staff terancam	Proses bisnis terganggu	10

ID	Kategori Asset	Nama Asset	Penyebab	Risk-ID	Risiko	Occ	Dampak Langsung	Dampak terhadap Bisnis	Sev
RR-34	People	Staff	Loading area dilakukan di tempat terbuka	R-08	*Human error*	3	• Manipulasi data • Kebocoran informasi	• Menurunnya reputasi • Proses bisnis terganggu	5

Halaman ini sengaja dikosongkan

LAMPIRAN D.
VERIFIKASI PROSEDUR AUDIT

Halaman ini sengaja dikosongkan

Tabel D. 1 Verifikasi Dokumen Prosedur Audit P.1.1

Audit Prosedur		**ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan**			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
1	a, b	Pendefinisian perimeter keamanan	Perimeter keamanan harus didefinisikan, dan penentuan letak dan kekuatan dari masing-masing perimeter harus sesuai pada persyaratan keamanan aset dalam perimeter dan hasil penilaian risiko	*Physical security perimeter*	11.1.1
1	c, d	Penentuan letak dan kekuatan perimeter			
1	e, f, g	Penentuan perimeter keamanan dari risiko			
2	a, b	Atap eksterior, dinding dan lantai area harus dari konstruksi yang solid	Perimeter bangunan atau situs yang berisi fasilitas pengolahan informasi harus *physically sound* (yaitu tidak boleh ada kesenjangan dalam perimeter atau daerah mana kerusakan bisa dengan mudah terjadi); atap eksterior, dinding dan lantai area harus dari konstruksi yang solid dan semua pintu eksternal harus sesuai dilindungi terhadap akses yang tidak sah dengan mekanisme		
2	c	Perimeter bangunan harus *physically sound*			
2	d, e	Pelindungan pintu dari akses yang tidak sah			

Audit Prosedur		ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
			kontrol, (misalnya bar, alarm, kunci); pintu dan jendela harus terkunci		
3	a, c	Penyediaan meja resepsionis	Meja resepsionis yang dijaga atau hal lain untuk mengontrol akses fisik ke area atau bangunan harus disediakan; akses ke area dan bangunan harus dibatasi untuk petugas yang berwenang saja		
3	b, d	Pembatasan akses ke area			
4	a, b	Pembuatan pelindung fisik	Pelindung fisik, jika memungkinkan, harus dibangun untuk mencegah akses fisik tidak sah dan pencemaran lingkungan		
5	a, b	Pembuatan alarm untuk kebakaran	Semua pintu harus diberi alarm, dipantau dan diuji dalam hubungannya dengan dinding untuk menetapkan tingkat yang		

Audit Prosedur		ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
5	c, d	Dinding yang kuat terhadap kebakaran	diperlukan terhadap perlawanan api sesuai dengan standar regional, nasional dan internasional yang sesuai		
6	a, b, c	Pemasangan system pendeteksi yang cocok	Sistem pendeteksi penyusup yang cocok harus dipasang dan secara teratur diuji yang mencakup pintu dan jendela yang mungkin diakses; daerah kosong harus diamankan		
7	a, b, c	Pemisahan fasilitas pengolahan informasi	Fasilitas pengolahan informasi yang dikelola oleh organisasi harus secara fisik dipisahkan dari yang dikelola oleh pihak eksternal		

Tabel D. 2 Verifikasi Dokumen Prosedur Audit P.1.2

Audit Prosedur		**ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan**			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
1	a, b	Perijinan pengunjung	Tanggal dan waktu masuk dan kepergian dari pengunjung harus dicatat, dan semua pengunjung harus diawasi kecuali akses mereka telah disetujui sebelumnya; mereka hanya dapat diberikan akses untuk tujuan tertentu yang diijinkan. Identitas pengunjung harus disahkan oleh orang yang berhak	*Physical entry controls*	11.1.2
1	c, d	Pencatatan Tanggal dan waktu masuk dan kepergian dari pengunjung			
1	e	Pengamanan buku log fisik	Buku log fisik atau audit trail elektronik dari semua akses harus aman dijaga dan dipantau		
2	a, b	Pembatasan akses ke wilayah informasi rahasia dengan penera-pan control akses	Akses ke daerah-daerah di mana informasi rahasia diproses atau disimpan harus dibatasi untuk individu yang berwenang hanya dengan menerapkan kontrol akses yang sesuai, misalnya dengan menerapkan		

Audit Prosedur		ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
			mekanisme otentikasi dua faktor seperti kartu akses dan PIN rahasia		
3	a, b	Pengidentifikasian karyawan, kontraktor dan pihak eksternal yang ada	Seluruh karyawan, kontraktor dan pihak eksternal harus diminta untuk memakai beberapa bentuk identifikasi terlihat dan harus segera memberitahukan petugas keamanan jika mereka menghadapi pengunjung tidak dikawal dan siapa pun yang tidak memakai identifikasi terlihat		
3	c	Pengawasan terhadap pengunjung			
3	d, e	Pelaporan pengunjung yang tidak sesuai peraturan			
4	a, b, c	Pemberian hak akses terbatas untuk pihak eksternal	Tenaga pelayanan dukungan pihak eksternal harus diberikan akses terbatas untuk mengamankan daerah atau fasilitas pengolahan informasi rahasia hanya ketika diperlukan; akses ini harus disahkan dan dipantau		

Audit Prosedur		ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
5	a, b, c	Evaluasi hak akses	Hak akses untuk mengamankan area harus secara berkala dan diperbarui, dan dicabut bila diperlukan		

Tabel D. 3 Verifikasi Dokumen Prosedur Audit P.1.3

Audit Prosedur		ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
1	a, b, c, d	Peletakan fasilitas public untuk menghindari akses publik	Fasilitas penting harus diletakkan untuk menghindari akses oleh publik	*Securing offices, rooms and facilities*	11.1.3
2	a, c	Tidak memberikan indikasi mengenai tempat pemrosesan data	Jika dapat diaplikasikan, bangunan harus bebas dari gangguan dan memberikan indikasi minimal tujuan mereka, dengan		

Audit Prosedur		ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
2	b	Menjauhkan ruangan dari gangguan	tidak ada tanda-tanda yang jelas, di luar atau di dalam gedung, mengidentifikasi adanya kegiatan pengolahan informasi		
1	a, b	Peletakan fasilitas fisik sehingga tidak terlihat dan terdengar dari luar	Fasilitas harus dikonfigurasi untuk mencegah informasi atau kegiatan rahasia terlihat dan terdengar dari luar. Perisai elektromagnetik juga harus dipertimbangkan		
3	a, b, c, d				
4	a, b, c, d	Pengamanan direktori dan buku telepon	Direktori dan buku telepon internal yang menyimpan lokasi dari fasilitas pengolahan informasi rahasia tidak boleh mudah diakses siapa pun yang tidak sah		

Tabel D. 4 Verifikasi Dokumen Prosedur Audit P.1.4

Audit Prosedur		**ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan**			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. kontrol**
1	a, b, c, d	Pengendalian terhadap kerusakan dari bencana alam dan ancaman lain	Saran spesialis harus diperoleh tentang cara untuk menghindari kerusakan dari kebakaran, banjir, gempa bumi, ledakan, kerusuhan sipil dan bentuk lain dari bencana alam	*Protecting against external and environmental threats*	11.1.4
2	a, b, c				
3	a, b, c, d, e, f				

Tabel D. 5 Verifikasi Dokumen Prosedur Audit P.1.5

Audit Prosedur		**ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan**			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. kontrol**
1	a, b, c	Kesadaran aktivitas di daerah aman	Personel harus menyadari adanya, atau kegiatan dalam, daerah aman	*Working in secure areas*	11.1.5
2	a, b	Pengawasan aktivitas dalam area kerja	Pekerjaan tanpa pengawasan di daerah aman harus dihindari baik untuk alasan keamanan		

Audit Prosedur		ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. kontrol**
			dan untuk mencegah peluang untuk kegiatan berbahaya		
3	a, b, c	Pengamanan ruangan ketika ditinggalkam	Area aman yang kosong harus secara fisik terkunci dan secara periodic diperiksa		
4	a, b	Peraturan penggunaan peralatan rekaman	Fotografi, video, audio atau peralatan rekaman lainnya, seperti kamera di perangkat mobile, seharusnya tidak diperbolehkan, kecuali diizinkan		

Tabel D. 6 Verifikasi Dokumen Prosedur Audit P.1.6

Audit Prosedur		**ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan**			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
1	c, d	Pembatasan akses ke wilayah pengiriman dan pemuatan	Akses ke wilayah pengiriman dan pemuatan dari luar gedung harus dibatasi hanya untuk personel yang berwenang;	*Delivery and loading areas*	11.1.6
2	a, b	Perancangan wilayah pengiriman dan pemuatan untuk menghindari akses ke wilayah lainnya	Wilayah pengiriman dan pemuatan daerah harus dirancang agar pasokan dapat dimuat dan dibongkar tanpa personil pengiriman mendapatkan akses ke bagian lain dari bangunan		
3	a, b	Pengamanan wilayah pengiriman dan pemuatan	Pintu eksternal dari pengiriman dan pemuatan daerah harus diamankan ketika pintu internal dibuka		
4	a, b	Pemeriksaan barang masuk	Bahan yang masuk harus didaftarkan sesuai dengan prosedur manajemen aset saat masuk ke area kerja		
4	c	Pemeriksaan barang masuk	Bahan yang masuk harus diperiksa dan diperiksa untuk bahan peledak, bahan kimia		

Audit Prosedur		ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
			atau bahan berbahaya lainnya, sebelum pindah dari wilayah pengiriman dan pemuatan		
4	d, e, f	Pemeriksaan barang masuk	Bahan yang masuk harus diperiksa untuk bukti gangguan perjalanan. Jika gangguan tersebut ditemukan harus segera dilaporkan kepada petugas keamanan		
5	a, b	Pemisahan pengiriman barang masuk dan keluar	Pengiriman masuk dan keluar harus secara fisik terpisah, jika dimungkinkan		

Tabel D. 7 Verifikasi Dokumen Prosedur Audit P.2.1

Audit Prosedur		**ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan**			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
1	b, d, e	Peletakkan peralatan untuk pelindungan dari akses tidak sah	Peralatan harus diletakkan untuk meminimalkan akses yang tidak perlu ke daerah kerja	*Equipment siting and protection*	11.2.1
1	f	Peletakan peralatan dari risiko terlihat	Fasilitas pengolahan informasi yang menangani data sensitif harus diposisikan hati-hati untuk mengurangi risiko informasi dilihat oleh orang yang tidak berwenang selama penggunaannya		
1	g	Pengamanan fasilitas	Fasilitas penyimpanan harus diamankan untuk menghindari akses yang tidak sah		
2	a, b, c	Pengadopsian control untuk mengurangi risiko	Kontrol harus diadopsi untuk meminimalkan risiko potensial ancaman fisik dan lingkungan, misalnya pencurian, kebakaran, bahan peledak, asap, air (atau kegagalan pasokan air), debu, getaran, efek kimia, gangguan pasokan listrik, gangguan		

Audit Prosedur		ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan			
#*Proc*	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
			komunikasi, radiasi elektromagnetik dan vandalisme		
2	d	Perlindungan dari petir	Perlindungan dari petir harus diterapkan untuk semua bangunan dan filter proteksi petir harus dipasang untuk semua kekuatan yang masuk dan jalur komunikasi		
3	a, b, c	Pedoman makan, minum, dan merokok	Pedoman untuk makan, minum dan merokok di dekat fasilitas pengolahan informasi harus ditetapkan		
3	d	Pemantauan kondisi lingkungan	Kondisi lingkungan, seperti suhu dan kelembaban, harus dipantau untuk kondisi yang dapat mempengaruhi pengoperasian fasilitas pengolahan informasi		
4	a,b	Perlindungan barang	Barang yang membutuhkan perlindungan khusus harus dijaga untuk mengurangi tingkat umum perlindungan yang diperlukan		
		Perlindungan khusus	Penggunaan metode perlindungan khusus, seperti membran keyboard, harus		

Audit Prosedur		ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan			
#*Proc*	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
			dipertimbangkan untuk peralatan di lingkungan industri		
		Pelindungan peralatan pengolahan informasi	Peralatan pengolahan informasi rahasia harus dilindungi untuk meminimalkan risiko kebocoran informasi karena emanasi elektromagnetik		

Tabel D. 8 Verifikasi Dokumen Prosedur Audit P.2.2

Audit Prosedur		**ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan**			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. kontrol**
1	c, d	Penyesuaian peralatan pendukung	Penyesuaian dengan spesifikasi peralatan pabrik dan persyaratan hukum lokal	*Supporting utilities*	11.2.2
2	a, b	Penilaian peralatan pendukung	Penilaian secara teratur untuk kapasitas mereka untuk memenuhi pertumbuhan bisnis dan interaksi dengan utilitas pendukung lainnya		
3	a, b, c	Pemeriksaan peralatan pendukung	Pemeriksaan dan pengujian secara teratur untuk memastikan fungsi yang tepat		
4	a, b	Pemasangan alarm pendeteksi malfungsi	Jika perlu, beri alarm untuk mendeteksi malfungsi		
5	a, b, c	Pemberian routing yang beragam	Jika perlu, miliki beberapa feed routing fisik yang beragam		

Tabel D. 9 Verifikasi Dokumen Prosedur Audit P.2.3

Audit Prosedur		**ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan**			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
1	a	Pemasangan kabel daya dan telekomunikasi di bawah tanah	Kabel daya dan telekomunikasi ke fasilitas pengolahan informasi harus di bawah tanah, ketika memungkinkan, atau pemberian perlindungan alternatif yang memadai	*Cabling security*	11.2.3
1	b	Pemisahan kabel daya dan kabel telekomunikasi	Kabel listrik harus dipisahkan dari kabel komunikasi untuk mencegah gangguan		
2	a, b, c, d	Perlindungan kabel dari kerusakan dan kebocoran informasi	Untuk sistem sensitif atau kritis lanjut kontrol untuk dipertimbangkan termasuk: 1) instalasi saluran lapis baja dan mengunci ruangan atau kotak pada titik pemeriksaan dan pemutusan; 2) menggunakan perisai elektromagnetik untuk melindungi kabel;		

Audit Prosedur		ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
			3) inisiasi peembersihan teknis dan pemeriksaan fisik untuk perangkat yang tidak sah yang melekat pada kabel; 4) akses dikendalikan untuk patch panel dan ruang kabel.		

Tabel D. 10 Verifikasi Dokumen Prosedur Audit P.2.4

Audit Prosedur		ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
1	a, b	Pemeliharaan peralatan sesuai anjuran pemasok	Peralatan harus dipelihara sesuai dengan interval servis pemasok yang dianjurkan dan spesifikasi	*Equipment maintenance*	11.2.4
2	a, b	Perawatan sesuai kebijakan asuransi	Semua persyaratan perawatan yang dikenakan oleh kebijakan asuransi harus dipenuhi		

Audit Prosedur		ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
3	a, b, c	Pemeliharaan oleh pihak yang berwenang	Hanya personil pemeliharaan yang berwenang yang harus melakukan perbaikan dan layanan peralatan		
4	a, b, c	Pengendalian setelah pemeliharaan peralatan	Sebelum meletakkan peralatan kembali ke dalam tempat semual setelah perawatan, maka harus diperiksa untuk memastikan bahwa peralatan tersebut tidak ada kerusakan		
4	d	Penyimpanan catatan perawatan	Catatan perkiraan kesalahan atau kesalahan aktual, dan semua pemeliharaan preventif dan korektif harus disimpan		
5	a, b	Pengendalian saat pemeliharaan peralatan	Pengendalian yang tepat harus dilaksanakan bila peralatan dijadwalkan untuk pemeliharaan, dengan mempertimbangkan apakah perawatan ini dilakukan oleh personel		

Audit Prosedur		ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan			
#*Proc*	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
6	a, b		internal atau eksternal organisasi; bila perlu, informasi rahasia harus dibersihkan dari peralatan atau personil pemeliharaan harus cukup jelas		

Tabel D. 11 Verifikasi Dokumen Prosedur Audit P.2.5

Audit Prosedur		ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan			
#*Proc*	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
2	a, b, c	Identifikasi personel yang memiliki izin pemindahan	Karyawan dan pihak eksternal yang memiliki otoritas untuk mengizinkan penghapusan off-site aset harus diidentifikasi	*Removal of assets*	11.2.5
3	a, b	Pencatatan pemindah aset	Identitas, peran dan afiliasi dari siapa saja yang menangani atau menggunakan aset harus didokumentasikan dan dokumentasi ini		

Audit Prosedur		ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
			kembali dengan peralatan, informasi atau perangkat lunak		
3	c	Pencatatan batas waktu penghapusan aset	Batas waktu untuk penghapusan aset harus ditetapkan dan kembali diverifikasi untuk kepatuhan		
3	a, d	Pencatatan aset yang dipindahkan	Bila perlu, aset harus dicatat sebagai aset yang dihapus off-site dan dicatat ketika kembali		

Tabel D. 12 Verifikasi Dokumen Prosedur Audit P.2.6

Audit Prosedur		**ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan**			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
1	a, b, c	Pengamanan peralatan *off-site*	Peralatan dan media diambil dari tempat tidak boleh dibiarkan tanpa pengawasan di tempat umum	*Security of equipment and assets off-premises*	11.2.6
1	d, e	Perlindungan peralatan *off-site*	Instruksi manufaktur untuk melindungi peralatan harus diamati setiap saat, misalnya perlindungan terhadap paparan medan elektromagnetik yang kuat		
2	a, b, c	Pencatatan peralatan *off-site*	Ketika peralatan *off-site* ditransfer antara individu-individu yang berbeda atau pihak eksternal, log harus dipertahankan yang mendefinisikan lacak balak untuk peralatan termasuk setidaknya nama dan organisasi dari orang-orang yang bertanggung jawab untuk peralatan		

Audit Prosedur		ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
3	a, b	Kontrol terhadap lokasi *off-site*	Kontrol untuk lokasi *off-site*, seperti rumah-kerja, teleworking dan situs sementara harus ditentukan oleh penilaian risiko dan kontrol cocok diterapkan sebagaimana mestinya, misalnya lemari arsip dikunci, kebijakan meja yang jelas, kontrol akses untuk komputer dan komunikasi yang aman dengan kantor		

Tabel D. 13 Verifikasi Dokumen Prosedur Audit P.2.7

Audit Prosedur		**ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan**			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
2	a, b, c	Penghapusan media informasi dengan metode khusus	Peralatan harus diverifikasi untuk memastikan apakah media penyimpanan yang terkandung sebelum dibuang atau digunakan kembali. Media penyimpanan yang berisi informasi rahasia atau hak cipta harus secara fisik dihancurkan atau informasinya harus dihancurkan, dihapus atau ditimpa menggunakan teknik untuk membuat informasi asli tidak dapat diambil kemabali daripada menggunakan standar menghapus atau fungsi Format	*Secure disposal or re-use of equipment*	11.2.7
3	a, b	Penghapusan informasi sebelum penghancuran peralatan			

Tabel D. 14 Verifikasi Dokumen Prosedur Audit P.2.8

Audit Prosedur		**ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan**			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
2	a	Pemutusan sesi aktif saat ditinggalkan	Mengakhiri sesi aktif ketika selesai, kecuali bisa diamankan oleh mekanisme penguncian yang tepat, misalnya dilindungi password screen saver	*Unattended user equipment*	11.2.8
2	b	Log off PC ketika tidak digunakan	Log-off dari aplikasi atau layanan jaringan ketika tidak lagi dibutuhkan		
2	c, d	Pemberian password pada computer dan perangkat mobile	Mengamankan komputer atau perangkat mobile dari penggunaan yang tidak sah oleh kunci kunci atau kontrol yang setara, misalnya akses password, jika tidak digunakan		

Tabel D. 15 Verifikasi Dokumen Prosedur Audit P.2.9

Audit Prosedur		**ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan**			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
1	c, d	Penyimpanan informasi bisnis bila tidak diperlukan	Informasi bisnis yang sensitif atau kritis, misalnya di atas kertas atau media penyimpanan elektronik, harus terkunci (idealnya dalam bentuk yang aman atau lemari atau lainnya furnitur keamanan) bila tidak diperlukan, terutama ketika kantor dikosongkan.	*Clear desk and clear screen policy*	11.2.9
2	a, b, c	Log-off dari aplikasi atau layanan jaringan ketika tidak lagi dibutuhkan	Komputer dan terminal harus dibiarkan log off atau dilindungi dengan layar dan keyboard dengan penguncian password, mekanisme otentikasi pengguna tanda atau serupa ketika tanpa pengawasan dan harus dilindungi oleh kunci kunci, password atau kontrol lain jika tidak digunakan		
2	d	Pemberian password pada computer			

Audit Prosedur		ISO/IEC 27002:2015 Klausul 11 Keamanan Fisik dan Lingkungan			
#Proc	**# Audit Checklist**	**Poin Utama**	***Implementation Guide***	***Control Objective***	**No. Kontrol**
3	a, b, c	pembatasan penggunaan teknologi reproduksi	Penggunaan yang tidak sah dari mesin fotokopi dan teknologi reproduksi lainnya (misalnya scanner, kamera digital) harus dicegah		

LAMPIRAN E.
PERSETUJUAN DOKUMEN PANDUAN AUDIT

Halaman ini sengaja dikosongkan

LEMBAR PERSETUJUAN DOKUMEN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN

Nama Peneliti: Stephen Christian

Judul Tugas Akhir:

PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO/IEC 27002:2013 PADA DIREKTORAT SISTEM INFORMASI UNIVERSITAS AIRLANGGA

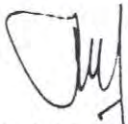
Deliverable:

1. Dokumen *Audit Plan*
2. Dokumen *Audit Program*
3. Dokumen Penggunaan Audit Program

Komentar:

Persetujuan:

Kepala Seksi Keamanan Data



Indri Sulistiyowati

Halaman ini sengaja dikosongkan

BIODATA PENULIS

Penulis bernama lengkap Stephen Christian. Penulis lahir di Malang, tanggal 24 September 1993 dan merupakan anak pertama dari tiga bersaudara. Penulis telah menempuh pendidikan formal di SD Negeri Sukun 7 Malang, SMP Negeri 3 malang, dan SMA Negeri 1 Malang.

Setelah lulus dari SMA pada tahun 2011, penulis diterima di Jurusan Sistem Informasi, Institut Teknologi Sepuluh Nopember Surabaya melalui jalur SNMPTN Tulis dan terdaftar dengan NRP 52 11 100 075. Selama masa perkuliahan, penulis aktif di bidang akademik dan non akademik. Dalam bidang akademik, penulis pernah menjadi asisten dosen di matakuliah Sitem Fungsional Bisnis I dan II, Pengelolaan Hubungan Pelanggan, Kalkulus dan Aljabar Linier, serta menjadi fasilitator unutk matakuliah Keterampilan Interpersonal. Dalam bidang non-akademik, penulis aktif dalam UKM Paduan Suara Mahasiswa ITS, ITS Expo 2011 bagian GKM, dan Manage Jurusan Sistem Informasi tahun 2012/2013.

Pada akhir semester akhir perkuliahan, penulis mengambil bidang minat Perencanaan dan Pengembangan Sistem Informasi dengan fokus topik Tugas Akhir Audit Teknologi Informasi. Untuk kepentingan penelitian, penulis dapat dihubungi melalui email yaitu stephentian93@gmail.com.