TUGAS AKHIR – KS141501

PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO/IEC 27002:2013 PADA RUANG SERVER STIE PERBANAS SURABAYA

DESIGNING A RISK BASED AUDIT GUIDELINE FOR PHYSICAL AND ENVIRONMENTAL INFORMATION TECHNOLOGY SECURITY BASED ON ISO/IEC 27002:2013 AT SERVER ROOM OF STIE PERBANAS SURABAYA

I PUTU ADI WIRANATA
NRP 5212 100 033

Dosen Pembimbing
Dr. Apol Pribadi Subriadi, S.T, M.T
Anisah Herdiayanti, S.Kom, M.Sc., ITIL

Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2017

TUGAS AKHIR – KS14 1501

PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO/IEC 27002:2013 PADA RUANG SERVER STIE PERBANAS SURABAYA

I PUTU ADI WIRANATA
NRP 5212 100 033

Dosen Pembimbing
Dr. Apol Pribadi Subriadi, S.T, M.T
Anisah Herdiayanti, S.Kom, M.Sc., ITIL

Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2017

FINAL PROJECT – KS 141501

DESIGNING A RISK BASED AUDIT GUIDELINE FOR PHYSICAL AND ENVIRONMENTAL INFORMATION TECHNOLOGY SECURITY BASED ON ISO/IEC 27002:2013 AT SERVER ROOM OF STIE PERBANAS SURABAYA

I Putu Adi Wiranata
5212 100 033

Academic Promotors
Dr. Apol Pribadi Subriadi, S.T, M.T
Anisah Herdiyanti, S.Kom, M.Sc., ITIL

INFORMATION SYSTEMS DEPARTMENT
Information Technology Faculty
Sepuluh Nopember Institut of Technology
Surabaya 2017

LEMBAR PENGESAHAN

PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO/IEC 27002:2013 PADA RUANG SERVER STIE PERBANAS SURABAYA

TUGAS AKHIR

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

Oleh:

I Putu Adi Wiranata
5212 100 033

Surabaya, Januari 2017

KETUA
JURUSAN SISTEM INFORMASI

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

LEMBAR PERSETUJUAN

PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO/IEC 27002:2013 PADA RUANG SERVER STIE PERBANAS SURABAYA

TUGAS AKHIR

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

Oleh:

I Putu Adi Wiranata
5212 100 033

Disetujui Tim Penguji : Tanggal Ujian : Januari 2017
Periode Wisuda : Maret 2017

Dr. Apol Pribadi Subriadi, S.T., M.T **(Pembimbing 1)**

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

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

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

PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO/IEC 27002:2013 PADA RUANG SERVER STIE PERBANAS SURABAYA

Nama Mahasiswa	**: I Putu Adi Wiranata**
NRP	**: 5212 100 033**
Jurusan	**: Sistem Informasi FTIf-ITS**
Dosen Pembimbing 1	**: Dr. Apol Pribadi Subriadi, S.T, M.T**
Dosen Pembimbing 2	**: Anisah Herdiyanti, S.Kom., M.Sc., ITIL**

ABSTRAK

Dalam pengelolaan teknologi informasi, keamanan merupakan salah satu aspek penting yang harus diperhatikan dan direncanakan untuk mengantisipasi ancaman yang muncul. Salah satu ancaman TI yang dampaknya cukup signifikan adalah ancaman yang datang dari alam, seperti yang baru saja dialami oleh STIE Perbanas Surabaya pada Juli 2015 kemarin dimana ruang server yang dimilikinya mengalami kebakaran.

Hal ini menunjukan pengendalian atau praktek keamanan informasi dan teknologi informasi pada ruang server tersebut masih kurang efektif dalam pelaksanaannya. Institute of Education Sciences mengatakan bahwa Physical Security merupakan bagian yang sangat penting dari sebuah rencana keamanan dan merupakan dasar untuk semua upaya keamanan yang ada. Keamanan fisik dan lingkungan mengacu pada perlindungan terhadap bangunan dan juga semua perlengkapannya dari ancaman. Salah satu standar dalam manajemen keamanan informasi yang memiliki klausul tersendiri dalam bidang keamanan fisik dan lingkungan adalah ISO/IEC 27002:2013. Untuk memastikan bahwa upaya keamanan telah dilakukan sesuai dengan standar yang sudah

ditetapkan, maka perlu dilakukan proses pengecekan. Salah satu pendekatan yang dapat digunakan untuk melakukan hal tersebut adalah dengan proses audit teknologi informasi. Dalam pelaksanaan proses audit, diperlukan sebuah bakuan atau panduan agar proses audit yang dilakukan nantinya dapat lebih terstruktur dan sesuai dengan standar untuk pelaksanaan audit. Dari permasalahan ini, maka dibutuhkan sebuah dokumen panduan audit teknologi informasi terutama untuk keamanan fisik dan lingkungan ruang server milik STIE Perbanas Surabaya.

Penyusunan dokumen panduan audit TI dimulai dengan penentuan template dari audit plan dan juga audit program yang akan digunakan. Selanjutnya dilakukan proses penggalian data dan informasi yang diperlukan dalam pembuatan panduan audit. Indentifikasi aset informasi yang kemudian dilakukan identifikasi terhadap risikonya dan penilaian berdasarkan metode FMEA untuk mendapatkan risiko dengan kategori High. Kemudian risiko akan dipetakan ke dalam control objective ISO/IEC 27002:2013 yang digunakan sebagai dasar dalam pembuatan program audit.

Luaran dari tugas akhir ini adalah dokumen panduan audit berbasis risiko yang berisikan Audit Plan dan Audit Program yang mengacu pada ISO/IEC 27002:2013 untuk keamanan fisik dan lingkungan. Dengan adanya dokumen panduan audit ini, nantinya diharapkan dapat membantu pihak STIE Perbanas Surabaya dalam mengecek pelaksanaan kontrol untuk keamanan informasi yang sudah diterapkan khususnya pada pengamanan ruang servernya.

Kata Kunci : Phisical Security, Keamanan Fisik dan Lingkungan, Audit TI, Audit Berbasis Risiko, ISO/IEC 27002:2013, Panduan Audit

DESIGNING A RISK BASED AUDIT GUIDELINE FOR PHYSICAL AND ENVIRONMENTAL INFORMATION TECHNOLOGY SECURITY BASED ON ISO/IEC 27002:2013 AT SERVER ROOM OF STIE PERBANAS SURABAYA

Name	**: I Puru Adi Wiranata**
NRP	**: 5212 100 033**
Departement	**: Sistem Informasi FTIf-ITS**
Supervisor 1	**: Dr. Apol Pribadi Subriadi, S.T, M.T**
Supervisor 2	**: Anisah Herdiyanti, S.Kom., M.Sc.**

ABSTRACT

In management of information technology, security is one of the important aspect that must be considered and planned to anticipate the emerging threats. One of IT threats which impact is quite significant is the threat that comes from nature, as recently experienced by Perbanas Surabaya in July 2015, where its server room was caught on fire.

This shows the information and information technology control or security practices in the server room is still less effective in its implementation. Institute of Education Sciences said that the Physical Security is a very important part of a security plan and it is the foundation for all security efforts. Physical and environmental security refers to the protection of the building and also all the equipment from threats. One of standards in information security management that discuss about physical security and the environment is ISO / IEC 27002: 2013. To ensure that security measures have been carried out in accordance with the standards that have been defined, it is necessary to do the checking process. We can do that with information technology audit process. In the implementation of the audit process, it takes a codification or guidelines so that the audit process will be more structured and in accordance

with the standards for the conducting audits. From this issue, it needed a guidance for information technology audit especially for physical and environmental security for the server room of Perbanas Surabaya.

Preparation of IT audit guidance begins with the determination of the template from the audit plan and audit program that will be used. Then gathering the data and information that required to make the audit guidance. Identify the IT assets and then identify the risk and make assessment using FMEA methods to get risk in high categories. Then the risk will be mapped to the control objectives of ISO / IEC 27002: 2013, which is used as a basis for the making of audit program.

The results of this thesis is a risk-based audit guidance that contains audit Audit Plan and Audit Program based on ISO / IEC 27002: 2013 for the physical and environment security. With this audit guidance, it is expected to assist Perbanas Surabaya in checking the implementation of controls for information security that has been applied in particular to the security of the server room.

Keywords : Physical Security, Physical and Environmental Security, IT Audit, Risk-Based Audit, ISO / IEC 27002: 2013, Audit Guidance

KATA PENGANTAR

Segala puji syukur penulis panjatkan kehadapan Tuhan Yang Maha Esa karena atas rahmat-Nya semata penulis dapat menyelesaikan Tugas Akhir dengan judul :

PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO/IEC 27002:2013 PADA RUANG SERVER STIE PERBANAS SURABAYA

sebagai salah satu syarat kelulusan untuk emperoleh gelar Sarjana Komputer di Jurusan Sistem Informasi – Institut Teknologi Sepuluh Nopember Surabaya.
Penulis menyadari bahwa dalam penyelesaian Tugas Akhir ini tidak terlepas dari doa, dukungan dan bantuan dari banyak pihak. Oleh sebab itu, pada kesempatan kali ini penulis ingin menyampaikan rasa terima kasih yang sebesar – besarnya kepada :

1. I Made Gatra dan Ni Nyoman Yastri, yang merupakan orang tua dari penulis yang salalu memberikan dukungan baik dalam bentuk doa, semangat maupun materi untuk menyelesaikan Tugas Akhir ini. Terima kasih yang sebesar – besarnya atas kerja keras dan dukungannya sehingga penulis dapat menempuh jenjang pendidikan hingga sejauh ini.
2. Bapak Dr. Apol Pribadi Subriadi, S.T., M.T., dan juga Inu Anisah Herdiyanti, S.Kom., M.Sc., ITIL, selaku dosen pembimbing yang telah meluangkan banyak waktu untuk membimbing dan memberikan motivasi kepada penulis untuk menyelesaikan Tugas Akhir ini.
3. Bapak Sholiq, S.T., M.Kom., M.SA , M.Kom., dan Ibu Amna Shifia Nisafani, S.Kom., M.Sc., yang telah bersedia

menjadi dosen penguji dan memberikan banyak masukan kepada penulis.

4. Ketua Jurusan Sistem Informasi ITS, Bapak Dr. Ir. Aris Tjahyanto, M.Kom.
5. Bapak Arif Wibisono, S.Kom., M.Kom., selaku dosen wali penulis yang senantiasa memberikan arahan serta motivasi selama penulis menempuh masa perkuliahan.
6. Ni Luh Komang Mariasih yang senantiasa memberikan semangat dan dukungan kepada penulis untuk menyelesaikan Tugas Akhir ini.
7. Bapak Hermono, selaku laboran dari laboratorium Manajemen Sistem Informasi yang banyaj membantu penulis dalam hal administrasi untuk penyelesaian Tugas Akhir
8. Teman – teman mahasiswa Jurusan Sistem Informasi angkatan 2012 yang sudah memberikan semangat dan dukungan untuk segera menyelesaikan Tugas Akhir.
9. Teman – teman anggota TPKH-ITS yang senantiasa memberikan dukungan dan semangat selama masa perkuliahan.
10. Pihak lainnya yang telah mendukung dan membantu penulis dalam kelancaran penyelesaian Tugas Akhir ini.

Penulis sangat menyadari bahwa penyusunan laporan untuk Tugas Akhir ini masih sangat jauh dari kata sempurna, oleh sebab itu kritik dan juga saran yang membangun untuk perbaikan kedepan sangat diharapkan penulis. Semoga buku Tugas Akhir ini dapat bermanfaat bagi semua pembacanya.

Surabaya, Desember 2016

Penulis

DAFTAR ISI

(halaman ini sengaja dikosongkan)

DAFTAR GAMBAR

Halaman ini sengaja dikosongkan

DAFTAR TABEL

BAB I
PENDAHULUAN

Pada bab ini dijelaskan beberapa hal mendasar dalam penulisan tugas akhir. Hal –hal yang mendasar meliputi latar belakang, rumusan permasalahan, batasan masalah, tujuan, dan manfaat dari tugas akhir. Dari uraian tersebut, diharapkan gambaran umum dari permasalahan dan pemecahan tugas akhir dapat dipahami.

1.1 Latar Belakang Masalah

Penggunaan komputer dan teknologi informasi lainnya pada masa sekarang ini menjadi hal yang dipandang penting oleh beberapa organiasi, instansi ataupun perusahaan termasuk juga instansi pendidikan. Penerapan TI sangat mendukung kinerja suatu organisasi, dimana inovasi TI sebagai sebuah faktor penting [1]. Selain itu, keuntungan yang diberikan dapat dirasakan dengan jelas ketika keputusan untuk menggunakan dan memanfaatkan teknologi informasi sudah sesuai dengan kebutuhan dan didukung oleh sumber daya manusia yang memadai. Terkait dengan penggunaan TI untuk mendukung bisnis suatu organisasi, salah satu permasalahan yang muncul adalah menyangkut tentang keamanan informasi dan juga teknologi informasi untuk memastikan kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaannya (*availability*) data serta informasi yang dimiliki. Keamanan informasi merupakan penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (*business continuity*), meminimalisir resiko bisnis (*reduce business risk*) dan juga memaksimalkan atau mempercepat pengembalian investasi serta peluang bisnis [2]. Sedangkan keamanan teknologi informasi merupakan usaha - usaha yang dilakukan untuk mengamankan infrastruktur teknologi informasi atau aset TI dari gangguan atau ancaman yang mungkin timbul. Masalah

keamanan merupakan salah satu aspek yang sangat penting untuk diperhatikan. Keamanan data dan informasi telah menjadi hal yang sangat penting terutama bagi perusahaan ataupun organiasasi yang menerapkan teknologi informasi sebagai pendukung proses bisnisnya.

Menurut *Institute of Education Sciences,* dalam menjaga keamanan informsi dapat dilakukan dengan menerapkan beberapa pengamanan, antara lain ; *Information Security, Software Security, User Access Security, Network (Internet) Security*, dan *Physical Security. Institute of Education Sciences* mengatakan bahwa *Physical Security* merupakan bagian yang sangat penting dari sebuah rencana keamanan dan merupakan dasar untuk semua upaya keamanan yang ada. Tanpa hal tersebut, *Information Security, Software Security, User Access Security*, dan *Network (Internet) Security* akan menjadi lebih sulit dan bahkan tidak memungkinkan. Keamanan fisik mengacu pada perlindungan terhadap bangunan dan juga semua perlengkapannya (*termasuk semua informasi dan perangkat lunak yang ada di dalamnya*) dari ancaman bencana alam (banjir, gempa bumi, angin rebut), kondisi dan perubahan lingkungan (suhu ekstrim, tingkat kelembaban tinggi, petir), tindakan pengerusakan yang disengaja (pencurian, vandalism, pembakaran), dan tindakan pengerusakan yang tidak disengaja (menumpahkan minuman, ventilasi udara yang buruk, kelebihan beban listrik).

Semua ancaman tersebut dapat diantisipasi dan diminimalisir dengan menerapkan atau mengimplementasikan seperangkat kontrol yang dapat berupa kebijakan dan prosedur. Strategi yang diterapkan untuk keamanan informasi dan TI memiliki fokus dan dibangun dengan tujuan tertentu yang disesuaikan dengan kebutuhan masing – masing. Salah satu acuan atau standar yang dapat digunakan untuk membuat kebijakan atau prosedur terkait dengan keamanan fisik dalam menjaga keamanan informasi dan teknologi informasi adalah ISO/IEC 27002 dimana pada standar ini memiliki satu klausul yang

khusus membahas keamanan fisik dan lingungan. ISO/IEC 27002 berisikan panduan yang menjelaskan contoh dalam penerapan keamanan informasi dengan menggunakan bentuk – bentuk kontrol dalam mencapai sasaran dari kontrol yang telah ditetapkan. Standar ini tidak mengharuskan bentuk – bentuk kontrol tertentu melainkan menyerahkannya kepada pihak pengguna untuk memeilih dan menerapkan kontrol yang tepat dan disesuaikan dengan kebutuhan, serta dengan mempertimbangkan hasil kajian risiko yang telah dilakukan. Selain itu, pengguna juga dapat memilih kontrol di luar daftar kontrol yang dimuat dalam standar ini selama sasaran dari kontrol tersebut dapat dipenuhi [3].

STIE Perbanas Surabaya merupakan salah satu instansi pendidikan yang sudah memanfaatkan teknologi informasi untuk mendukung proses bisnisnya. Hal ini dapat dilihat dari beberapa sistem informasi yang diimplementasikan untuk mendukung proses bisnis akademiknya. Pada Juli 2015 lalu, ruang server milik STIE Perbanas Surabaya mengalami kebakaaran. Hal ini tentu mengakibatkan kerugian karena aset informasi dan teknologi informasi berharga yang dimiliki oleh STIE Perbanas Surabaya berada pada ruangan tersebut. Melihat hal ini, pengendalian keamanan yang telah ditetapkan oleh STIE Perbanas Surabaya dalam upaya mencapai keamanan informasi dan teknologi informasi perlu diperiksa untuk melihat sejauh mana pengendalian keamanan tersebut sudah dilaksanakan. Salah satu pendekataan yang dapat digunakan adalah dengan melakukan proses audit teknologi informasi. Menurut penelitian yang dilakukan oleh Stephen [4], audit TI atau Audit SI (Sistem Informasi) adalah bentuk pemeriksaan dan pengendalian dari infrastruktur TI secara menyeluruh. Dalam melakukan proses audit TI, tentu diperlukan sebuah bakuan atau panduan agar proses audit yang dilakukan nantinya dapat lebih terstruktur dan sesuai dengan standar untuk pelaksanaan audit.

Penelitian Tugas Akhir ini bertujuan untuk menghasilkan sebuah panduan proses audit teknologi informasi untuk keamanan fisik dan pengendalian lingkungan TI pada ruang server STIE Perbanas Surabaya berdasarkan ISO/IEC 27002:2013. 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 [4]. Adapun hasil dari tugas akhir ini terdiri atas penjelasan mengenai tujuan, ruang lingkup, informasi auditee dan auditor, acuan dan penanggung jawab audit, prosedur udit, audit checklist, serta formulir lainnya yang dapat mendukung proses audit teknologi informasi.

1.2 Perumusan Masalah

Berdasarkan atas uraian dari latar belakang tersebut, maka rumusan permasalahan yang akan menjadi fokus untuk diselesaikan pada Tugas Akhir ini adalah sebagai berikut :

1. Apa yang menjadi risiko terkait dengan pengelolaan keamanan fisik dan lingkungan teknologi informasi pada ruang server STIE Perbanasa Surabaya?
2. Apa yang menjadi *control objective* dan panduan dalam implementasi yang dapat mencegah atau memitigasi risiko yang sudah teridentifikasi?
3. Seperti apa usulan *audit plan* yang dibuat?
4. Seperti apa usulan *audit program* yang dibuat?

1.3 Batasan Masalah

Dalam pengerjaan Tugas Akhir ini, terdapat beberapa hal yang menjadi batasan masalah yang harus diperhatikan, yaitu :

1. Aset yang dimaksud dalam proses identifikasi aset adalah aset yang berupa fisik dan berada pada ruang server milik STIE Perbanas Surabaya.

2. Dokumen panduan audit SI/TI yang dihasilkan akan berfokus pada aspek pengelolaan dan pengendalian Keamanan Fisik dan Lingkungan TI untuk aset di ruang server STIE Perbanas Surabaya.
3. Standar yang digunakan sebagai acuan dalam pembuatan panduan audit TI adalah ISO/IEC 27002:2013 klausul keamanan fisik dan lingkungan.
4. Dokumen panduan audit SI/TI berfokus pada dua bagian yaitu Dokumen *Audit Plan* dan *Audit Program.*

1.4 Tujuan Tugas Akhir

Penelitian Tugas Akhir ini bertujuan untuk menghasilkan sebuah panduan audit teknologi informasi untuk keamanan fisik dan lingkungan TI pada ruang server STIE Perbanas Surabaya berdasarkan ISO/IEC 27002:2013. Adapun hasil dari tugas akhir ini terdiri atas penjelasan mengenai tujuan, ruang lingkup, informasi auditee dan auditor, acuan dan penanggung jawab audit, prosedur udit, audit checklist, serta formulir lainnya yang mendukung proses audit TI.

1.5 Manfaat Tugas Akhir

Manfaat yang di dapat dengan Tugas Akhir ini adalah sebagai berikut :

1. STIE Perbanas Surabaya dapat memperoleh informasi mengenai aset – aset informasi dan teknologi informasi penting yang perlu dilindungi untuk menjaga keamanan informasinya.
2. Membantu pihak STIE Perbanas Surabaya dalam memperoleh informasi terkait dengan risiko Keamanan Fisik dan Lingkungan TI pada ruang server STIE Perbanas Surabaya sehingga dampak yang dapat diakibatkan dapat diminimalisir.
3. Membantu pihak STIE Perbanas Surabaya dalam melakukan proses audit secara lebih terstruktur.

1.6 Relevansi

Topik yang diangkat pada pembuatan Tugas Akhir ini adalah Pembuatan Panduan Audit Kemanan Fisik dan Lingkuangan Teknologi Informasi Berbasis Risiko Berdasarkan ISO/IEC 27002;2013 dengan studi kasus ruang server STIE Perbanas Surabaya. Tugas Akhir ini berkaitan dengan mata kuliah Audit SI/TI dan juga Manajemen Risiko SI/TI yang termasuk dalam ruang lingkup penelitian pada laboratorium Manajemen Sistem Informasi.

BAB II
TINJAUAN PUSTAKA

Pada bab ini akan dijelaskan tentang tinjauan pustaka yang berkaitan dengan tugas akhir yang terdiri dari penelitian sebelumnya dan dasar teori.

2.1 Penelitian Sebelumnya

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

Tabel 2.1 Perbandingan Penelitian Sebelumnya

	Penelitian 1	**Penelitian 2**	**Penelitian 3**
Nama Peneliti	Stephen Christian (2015)	Mochammad Arief Ramadhan (2011)	Yudhis Cahyo Eko (2013)
Judul Penelitian	Pembuatan Panduan Audit Kemanan Fisik dan Lingkungan Teknologi Informasi Berbasis Risiko Berdasarkan ISO/IEC 27002:2013 Pada Direktorat Sistem Informasi Universitas Airlangga [4]	Pembuatan Perangkat Audit Internal TI Berbasis Risiko Menggunaan ISO/IEC 27002:2007 Pada Proses Pengelolaan Data Studi Kasus Digital Library ITS [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
Nama Peneliti	Stephen Christian (2015)	Mochammad Arief Ramadhan (2011)	Yudhis Cahyo Eko (2013)
Hasil Pnelitian	Penelitian ini berisi pembuatan perangkat audit yang berupa *audit plan* dan *audit program* yang mengacu pada ISO/IEC 27002:2013 pada Direktorat Sistem Informasi Universitas Airlangga. Klausul ISO/IEC 27002:20013 yang digunakan pada penelitian ini adalah *Physical and Environmental Security* yang memiliki 15 *control objective*.	Penelitian ini menghasilkan perangkat audit yang berupa *audit checklist* untuk Digital Library ITS. Perangkat audit yang dibuat mengacu pada ISO/IEC 27002:2007 dimana pada standar ini sudah terdapat acuan untuk standar pengelolaan keamanan.	Peneltian ini berisikan pembuatan panduan audit yang mengacu pada COBIT 5. Adapun panduan audit yang dibuat pada penelitian ini antara lain ikhtisar dokumen panduan audit, kertas kerja pemeriksaan utama, audit checklist, prosedur audit, dan kertas kerja konsep temuan.

	Penelitian 1	Penelitian 2	Penelitian 3
Nama Peneliti	Stephen Christian (2015)	Mochammad Arief Ramadhan (2011)	Yudhis Cahyo Eko (2013)
Kelebihan	Produk berupa perangkat audit yang dibuat pada penelitian ini cukup lengkap dan sudah disertai dengan persetujuan dari pihak Direktorat Sistem Informasi Universitas Airlangga sehingga kesesuaian antara perangkat audit yang dibuat dengan kebutuhan dari pihak Direktorat Sistem Informasi Universitas Airlangga dapat dipastikan.	Pemetaan risiko dilakukan dengan baik dan sudah mengacu pada ISO/IEC 27002:2007, sehingga dalam pembuatan perangkat audit yaitu *audit checklist* menjadi lebih mudah dan hasilnya lebih terstruktur.	*Framework* COBIT 5 ini mengintegrasikan beberapa *best pactice* teknologi informasi sehingga penilaian proses menjadi lebih efektif. Selain itu, COBIT 5 juga menjelaskan aktivitas apa saja yang harus dilakukan untuk memenuhi suatu *control objective*.

	Penelitian 1	Penelitian 2	Penelitian 3
Nama Peneliti	Stephen Christian (2015)	Mochammad Arief Ramadhan (2011)	Yudhis Cahyo Eko (2013)
Kekurangan	Proses analisa risiko pada penelitian ini dilakukan oleh peneliti dengan persetujuan dari pihak Direktorat Sistem Inforamsi Universitas Airlangga. Hal ini akan lebih maksimal jika pihak Direktorat Sistem Inforamsi Universitas Airlangga sudah memiliki dokumen terkait manajemen risiko dan kontrol – kontrol tertentu yang dapat digunakan oleh penulis.	Hasil dari penelitian yang berupa produk perangkat audit hanya sebatas *audit checklist* saja. Sehingga jika perangkat audit ini digunakan, hasil yang diperoleh hanya sebatas sesuai atau tidaknya temuan dengan *checklist* yang ada tanpa diikuti rekomendasi ataupun tinjauan dari auditor.	Panduan audit yang sudah dibuat hanya diverifikasi kelengkapannya saja oleh pihak KPPN II sehingga masih ada kemungkinan ketidaksesuaian antara isi dari panduan audit yang sudah dibuat dengan kebutuhan dari KPPN II.

	Penelitian 1	Penelitian 2	Penelitian 3
Nama Peneliti	Stephen Christian (2015)	Mochammad Arief Ramadhan (2011)	Yudhis Cahyo Eko (2013)
Relevansi Penelitian	Fokus penelitian yang akan dilakukan adalah membuat panduan audit dan pada penelitian 1 ini, produk berupa panduan audit yang dihasilkan dapat digunakan sebagai salah satu acuan untuk memudahkan penulis dalam pembuatan panduan audit yang berisikan *audit plan* dan *audit program*.	Penulis menggunakan penelitian ini untuk membantu dalam pengerjaan Tugas Akhir khususnya dalam pembuatan *checklist* serta pemetaan risiko yang mengacu pada ISO/IEC 27002 dengan harapan pemetaan risiko nantinya menjadi lebih terstruktur dan tepat.	Penulis dapat menggunakan penelitian ini untuk membantu dalam penyelesaian Tugas Akhir karena pada penelitian ini juga membahas tentang keamanan lingkungan fisik sehingga aktivitas yang harus dilakukan untuk memenuhi suatu *control objective* dari penelitian ini dapat digunakan.

2.2 Dasar Teori

Pada bagian ini, peneliti akan memaparkan dasar teori yang terkait dengan penelitian yang dilakukan oleh peneliti.

2.2.1 Pengertian Audit

Audit merupakan suatu istilah yang sering dipergunakan dalam bidang ekonomi. Secara umum, audit memiliki arti sebagai sebuah kegiatan pemeriksaan. Audit merupakan pemeriksaan laporan keuangan perusahaan oleh perusahaan akuntan publik yang independen. Audit ini terdiri dari penyelidikan terkait catatan akuntansi dan bukti lain yang mendukung laporan keuangan tersebut. Dengan memperoleh pemahaman tentang pengendalian internal perusahaan, dan dengan memeriksa dokumen, mengamati aset, membuat pertanyaan dalam dan di luar perusahaan, serta melakukan prosedur audit lainnya, auditor akan mengumpulkan bukti yang diperlukan untuk menentukan apakah laporan keuangan menyediakan gambaran keadaan finansial perusahaan yang wajar dan cukup lengkap dan kegiatannya selama periode yang diaudit [7].

Menurut Alvin A. Arens, Mark S. Beasley dan Randal J.Elder [8], audit adalah pengumpulan dan pengevaluasian bukti terkait informasi untuk menentukan dan melaporkan tingkat kesesuaian antara informasi dan kriteria yang ditetapkan. Auditing harus dilakukan oleh pihak yang kompeten dan independen.

Sedangkan pengertian audit menurut *The American Accounting Association's Committee on Basic Auditing Concepts*, audit merupakan suatu proses sistematis yang dilakukan untuk mendapatkan serta mengevaluasi bukti secara obyektif terkait dengan suatu pernyataan tentang kegiatan dan kejadian ekonomi dengan tujuan untuk menetapkan tingkat kesesuaian antara pernyataan - pernyataan tersebut dengan kriteria yang

telah ditetapkan, serta menyampaikan hasilnya kepada pihak yang berkepentingan.

Jadi, dapat disimpulkan bahwa audit merupakan serangkaian pemeriksaan terhadap semua bukti yang ditemukan terkait dengan proses yang sudah berlangsung atau dilakukan sebelumnya, dengan tujuan untuk menemukan ketidaksesuaian antara proses yang sudah berjalan dengan standar yang telah ditetapkan, kemudian menyampaikan hasilnya kepada pihak yang berkepentingan.

2.2.2 Pengertian Audit SI/TI

Audit Sistem Informasi atau Teknologi Informasi merupakan proses pemeriksaan terhadap bukti (*evidence*) untuk menemukan apakah sistem informasi dan semua infrastruktur teknologi informasi yang dimiliki sudah bisa melindungi aset serta mampu menjaga integritas data dan informasi sehingga dapat mendukung organisasi dalam mencapai tujuan bisnis secara efektif. Pada buku "*Information System Controls and Audit"*[9], disebutkan beberapa alasan pentingnya audit teknologi informasi, diantaranya :

1. Kerugian akibat kehilangan data
   Adanya gangguan dari virus atau terjadi insiden kebakaran pada ruangan tempat komputer berada akan mengakibatkan hilangnya seluruh data. Kehilangan data akan mempersulit perusahaan bahkan tidak memungkinkan untuk melakukan pengecekan data.

2. Kesalahan dalam pengambilan keputusan
   Saat ini terdapat cukup banyak pengusaha yang telah menggunakan bantuan dari *Decision Support System* (DSS) dalam mengambil keputusan - keputusan bisnis yang bersifat krusial atau penting. Risiko yang bisa saja terjadi adalah ketika salah memasukkan data ke dalam sistem yang akan mengarahkan pengguna kepada pengambilan keputusan yang kurang tepat atau bahkan tidak tepat.

3. Risiko kebocoran data
   Bagi sebagian besar pelaku usaha, data merupakan salah satu sumber daya yang tidak ternialai harganya. Kebocoran data terntu akan memberikan dampak besar yang dapat mengganggu keberlangsungan bisnis perusahaan.
4. Besarnya nilai investasi perangkat keras dan perangkat lunak.
   Biaya, modal, atau investasi yang dikeluarkan untuk sebuah proyek teknologi informasi seringkali bernilai sangat besar. Pada salah satu penelitian yang pernah dilakukan [10], mengatakan bahwa 20% pengeluaran TI terbuang secara percuma, 30 - 40% proyek TI tidak mendatangkan keuntungan. Selain itu, manfaat yang dapat diberikan oleh TI sangat sulit untuk diukur.

2.2.3 Audit Keamanan Informasi

Audit keamanan informasi merupakan suatu proses atau kegiatan yang memiliki basis pada kebijakan atau standar keamanan untuk menentukan semua keadaan dari perlindungan yang ada, dan untuk memverifikasi apakah perlindungan yang ada telah berjalan dengan baik dan sesuai. Target dari audit ini adalah untuk menemukan apakah lingkungan yang ada sekarang telah aman dilindungi sesuai dengan kebijakan keamanan yang sudah ditetapkan sebelumnya. Untuk menjaga independensi hasil, audit kemanan informasi harus dilaksanakan oleh pihak ketiga yang terpercaya dan juga independen [11].

Pada audit keamanan informasi terdapat kontrol yang dapat dikategorikan menjadi tiga yaitu ; teknis, fisik dan juga administrasi [12]. Dari ketiga jenis kontrol tersebut dapat dikategorikan lagi menjadi dua yaitu yang bersifat dan yang bersifat *preventive*. Beberapa jenis kontrol yang diaudit pada

audit kemanan informasi dapat dilihat pada Tabel 2.2 di bawah ini.

Tabel 2.2 Kontrol Audit Keamanan Fisik

	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 review	• Security reviews and audits • Performance evaluations • Required vacations/rotation of duties • Incident investigations

2.2.4 Proses Audit

Berdasarkan ISO 19011 [13], Proses Audit terdiri atas :

1. *Initiating the Audit*

   Ketika sebuah audit dimulai, tanggung jawab atas keberlangsungan audit berada di tangan ketua tim audit seperti yang ditetapkan pada audit program hingga audit tersebut selesai. Untuk memulai audit, langkah-langkah berikut harus dipertimbangkan, namun urutannya dapat berbeda tergantung pada *auditee*, proses dan situasi tertentu.

   Pada tahap awal memulai audit, terdapat 2 hal yang perlu untuk diperhatikaan yaitu :

   1.1 Pertemuan Awal dengan *Auditee*

   Pertemuan awal dengan auditee ini harus dilakukan oleh ketua tim audit baik secara formal maupun informal. Tujuan dari pertemuan awal ini antara lain untuk membangun jaringan komunikasi dengan perwakilan auditee, mengkonfirmasi kewenangan untuk melaksanakan audit, dan memberikan semua informasi mengenai audit yang akan dilaksanakan termasuk ruang lingkup, metode, tim audit, auditee, hingga jadwal.

   1.2 Menentukan Kemungkinan Audit

   Kemungkinan dari sebuah audit menentukan apakah semua sumberdaya, informasi, dan pengaturan yang diperlukan dapat menunjukan bahwa tujuan dari audit bisa tercapai. Kemungkinan dari audit harus ditentukan agar ketika tujuan audit yang akan dilaksanakan terlihat tidak memungkinkan, auditor dapat mengajukan perubahan kepada *client* dengan persetujuan dari *auditee.*

2. *Preparing Audit Activities*

   Hal – hal yang perlu diperhatikan dalam tahapan persiapan aktivitas audit ini antara lain :

   2.1 Meninjau Dokumen Sistem Manajemen untuk Persiapan Audit

Proses ini bertujuan agar auditor dapat mengumpulkan semua informasi yang diperlukan untuk dapat dipergunakan pada audit selanjutnya. Dokumen yang harus ditinjau antara lain dokumen sistem manajemen beserta semua catatannya dan laporan audit sebelumnya.

2.2 Menyiapkan Dokumen *Audit Plan*

Ketua tim audit harus menyiapkan rencana audit berdasarkan informasi yang terkandung dalam program audit dan dokumentasi yang diberikan oleh *auditee*. Rencana audit harus mempertimbangkan efek dari audit tersebut pada pihak *auditee* dan memberikan dasar bagi kesepakatan antara klien audit, tim audit dan auditee terkait pelaksanaan audit tersebut. Rencana tersebut harus memfasilitasi penjadwalan yang efisien dan koordinasi kegiatan audit untuk mencapai suatu hasil yang efektif.

Audit plan harus mencakup dan mengacu pada hal – hal berikut ini :

a. Tujuan audit
b. Ruang lingkup audit
c. Kriteria audit
d. Lokasi, tanggal, waktu yang direncanakan serta durasi pelaksanaan audit termasuk juga rapat dengan pihak manajeman *auditee*
e. Metode audit yang digunakan
f. Peran dan tanggunng jawab anggota tim audit

Audit plan harus dipresentasikan, dintinjau dan disetujui oleh *auditee* sebelum aktivitas audit dimulai. Kerancuan apapun pada *audit plan* harus diselesaikan antara *auditee*, *audit client*, dan *auditor.*

2.3 Penugasan Tim Audit

Ketua tim audit berkonsultasi dengan tim audit, dalam memberikan tanggung jawab kepada setiap anggota tim audit untuk melakukan audit pada

proses, fungsi, lokasi, atau aktivitas tertentu. *briefing* tim audit yang seharusnya diselenggarakan secara teratur oleh ketua tim audit, harus mengalokasikan tugas kerja dan memutuskan perubahan yang memungkinkan. Perubahan pada tugas kerja dapat dilakukan saat audit sedang berlangsung untuk memastikan pencapaian tujuan audit.

2.4 Menyiapkan Dokumen Kerja

Anggota tim audit harus meninjau informasi yang relevan dengan tugas audit mereka dan mempersiapkan dokumen kerja yang diperlukan untuk referensi dan untuk mencatat bukti audit. Dokumen kerja tersebut harus mencakup :

a. *Checklist*
b. Rencana *audit sampling*
c. Formulir untuk pencatatan bukti audit, temuan audit, dan catatan rapat.

3. *Conducting the Audit Activities*

Pelaksanaan aktivitas audit biasanya meliputi hal – hal berikut ini :

a. Melakukan *kick-off meeting*
b. Melakukan peninjauan 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 kesimpulan audit
h. Melakukan *closing meeting*

4. *Preparing and Distributing the Audit Report*

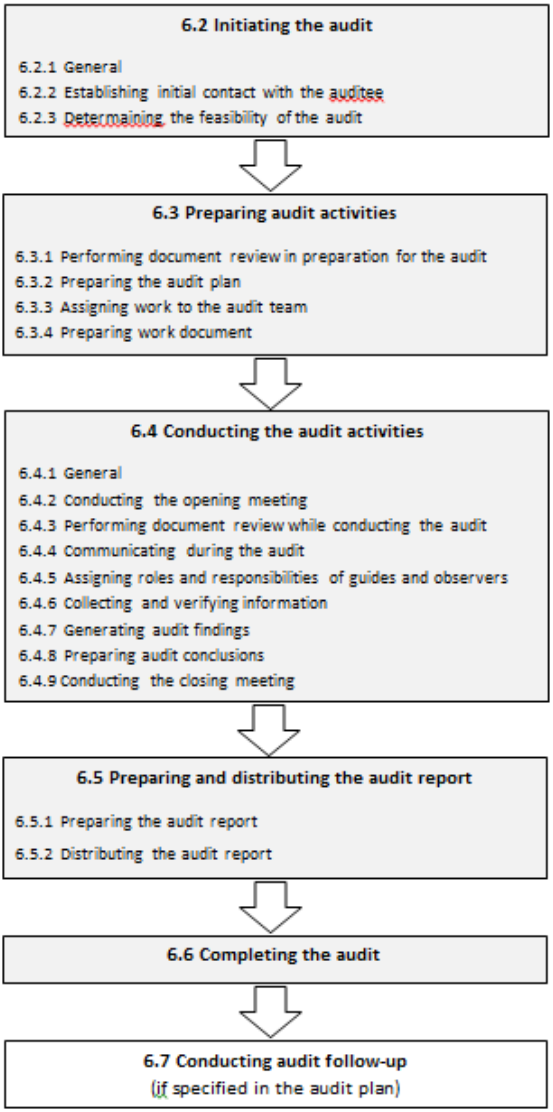
Ketua tim audit harus bertanggung jawab atas penyusunan dan isi laporan audit. Laporan audit harus memberikan catatan yang lengkap, akurat, ringkas dan jelas dari audit yang sudah dilaksanakan. Laporan audit

harus dikeluarkan dalam suatu periode waktu yang disepakati. Jika tertunda, alasannya harus dikomunikasikan kepada auditee dan pihak yang bertanggung jawab untuk mengelola program audit. Laporan audit harus tertanggal, dan disetujui sesuai sesuai dengan prosedur program audit. Kemudian laporan audit harus didistribusikan kepada penerima sebagaimana didefinisikan dalam prosedur audit.

5. *Completing the Audit*
   Audit dikatakan selesai ketika semua rencana aktivitas audit telah dilakukan atau telah disetujui oleh pihak yang bertanggung jawab untuk mengelola program audit tersebut. Dokumen yang terkait dengan audit dapat disimpan atau dimusnahkan sesuai dengan kesepakatan antara pihak yang berpartisipasi dan sesuai dengan prosedur program audit dan persyaratan hukum serta persyaratan lainnya. Pembelajaran yang didapatkan selama proses audit harus dicatat dalam sistem manajemen organisasi yang diaudit.

6. *Conducting Audit Follow–Up*
   Kesimpulan dari audit yang telah dilakukan bisa saja tergantung pada tujuan audit, hal ini menunjukkan perlunya koreksi, perbaikan, tindakan pencegahan atau perbaikan. Tindakan tersebut biasanya diputuskan dan dilakukan oleh auditee dalam jangka waktu yang telah disepakati. Auditee juga harus menghubungi dan mengkomunikasikan kepada tim audit mengenai status kegiatan perbaikan yang dilakukan.

Untuk gambaran mengenai proses audit yang ada pada standar ISO 19011 [13], dapat dilihat pada Gambar 2.1.



Gambar 2.1 Proses Audit [13]

Dari semua proses audit yang ada pada ISO 19011 (proses 1–6), dalam pengerjaan Tugas Akhir ini, yang akan digunakan hanyalah proses 1 dan 2 yaitu *Initiating the Audit* dan *Preparing Audit Activities* dimana fokus dari kedua proses ini adalah persiapan (*planning*) dari kegiatan audit. Proses 3 samapai dengan proses 6 tidak akan dilaksanakan karena penulis tidak sampai pada tahapan melakukan proses audit.

2.2.5 Audit Berbasis Risiko

Menurut *Institute of Internal Auditor* (IIA), Audit Berbasis Risiko adalah metodologi yang menghubungkan audit internal dengan kerangka kerja manajemen risiko organisasi secara keseluruhan. Metodologi ini memungkinkan audit internal untuk memberikan jaminan kepada direksi bahwa proses manajemen risiko telah dikelola dengan baik dan efektif di dalam batasan risiko yang telah ditetapkan. 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.

2.2.6 Panduan Audit

Menurut Satriadi (2010), buku panduan merupakan 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.

Jadi, buku panduan audit adalah kumpulan kertas yang berisikan tulisan – tulisan yang berfungsi sebagai panduan bagi seorang auditor dalam melakukan proses audit yang dijilid dalam satu bentuk buku. Buku panduan audit ini bertujuan untuk membantu auditor dalam memahami proses dan juga

informasi selama audit berlangsung serta membantu auditor dalam melakukan proses audit yang lebih terstruktur.

Secara garis besar, panduan audit terdiri dari beberapa bagian yaitu [4] :

a. Dokumen *Audit Charter*
   Audit Charter adalah sebuah dokumen resmi yang berisikan tujuan, wewenang, dan tanggung jawab dari aktivitas audit internal. Posisi proses audit internal dalam organisasi ditetapkan dalam sebuah *Audit Charter*. Persetujuan akhir dari sebuah *Audit Charter* akan dilakukan dengan jajaran eksekutif.
b. Dokumen *Audit Plan*
   Audit Plan merupakan sebuah pedoman khusus yang harus diikuti ketika melakukan proses audit. *Audit Plan* menggambarkan semua proses yang harus dilakukan oleh auditor dalam mencapai tujuan dari audit yang akan dilaksanakan. Dokumen ini akan membantu auditor memperoleh bukti yang cukup serta tepat, membantu menjaga biaya audit pada tingkat yang wajar, dan membantu menghindari kesalahpahaman dengan klien atau pihak yang diaudit.

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

   - Tujuan audit
   - Ruang lingkup audit
   - Kriteria audit
   - Lokasi, tanggal, waktu yang direncanakan dan durasi audit dilaksanakan, termasuk rapat dengan pihak manajemen auditee
   - Metode audit yang akan digunakan
   - 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 ataupun dalam satu kombinasi.

Top Management harus memastikan bahwa tujuan program audit sudah ditetapkan dan menetapkan satu orang yang berkompeten atau lebih untuk mengelola program audit tersebut. 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.

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

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

Dalam penelitian yang dilakukan oleh penulis kali ini, dokumen panduan audit akan difokuskan pada *Audit Plan* dan *Audit Program* saja. Dokumen *Audit Program* akan mengacu pada hasil penelitian milik Stephen Christian [4] dengan beberapa penyesuaian. *Audit Program* yang disusun penulis akan berisikan hal – hal berikut ini :

- Tujuan serta ruang lingkup audit,
- Best practice dan kendali tujuan,

- Prosedur audit,
- Dokumen atau formulir kerja audit.

2.2.7 Aset Informasi

Aset Informasi merupakan sesuatu yang teridentifikasi dan juga dikelola sebagai sebuah unit informasi sehingga dapat dipahami, dibagi, dilindungi dan dimanfaatkan secara efektif. Aset Informasi dapat juga diartikan sebagai sepotong informasi yang terdefinisi, disimpan dengan cara apapun, tidak mudah untuk diganti tanpa biaya, keahlian, waktu, sumber daya dan kombinasinya serta diakui sebagai sesuatu yang berharga bagi organisasi yang memilikinya [14].

Keamanan aset informasi diklasifikasikan ke dalam tiga hal utama yaitu [15] :

1. *Confidential*
   Informasi yang sangat berharga bagi sebuah perusahaan. Jika informasi ini sampai bocor ke luar organisasi, maka akan mengakibatkan kerugian atau kehilangan citra dari perusahaan.
2. *Internal Use Only*
   Informasi yang hanya boleh diakses dan diketahui oleh pihak internal perusahaan. Contohnya informasi mengenai kebijakan, materi pelatihan dan yang lainnya.
3. *Public*
   Informasi dapat diakses dan diketahui oleh semua orang baik pihak internal maupun eksternal dari perusahaan. Informasi yang dipublis akan disetujui terlebih dahulu oleh pihak perusahaan.

Pada penelitian ini, aset informasi yang dimaksud adalah semua peralatan, aset informasi dan teknologi informasi termasuk juga infrastruktur teknologi informasi yang dimiliki oleh STIE Perbanas Surabaya yang dilindungi dan disimpan dalam sebuah ruang server.

2.2.8 Risiko SI/TI

Risiko merupakan variasi dalam hal-hal yang mungkin terjadi secara alami didalam suatu situasi [16]. Risiko adalah ancaman terhadap kehidupan, properti atau keuntungan finansial akibat bahaya yang terjadi [17]. Jadi, risiko merupakan segala macam bentuk ancaman atau hal buruk yang mungkin terjadi baik secara alami maupun tidak sehingga dapat mengancam aset ataupun properti yang memiliki nilai finansial.

Menurut George & Hunter (2007) risiko teknologi informasi adalah sebeuah kejadian yang tidak dapat direncanakan dan berdampak pada kegagalan atau penyalahgunaan teknologi informasi yang mengancam tujuan bisnis. Jadi risiko TI dapat dikatakan sebagai segala bentuk ancaman atau hal buruk yang dapat terjadi baik secara alami ataupun tidak terhadap aset teknologi informasi dari suatu perusahaan yang terlibat dan berpengaruh secara langsung terhadap tujuan bisnis perusahaan.

ISACA menerbitkan *IT Risk Framework* sebagai sebuah pandangan yang komprehensif terhadap risiko yang berkaitan 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 [4].

2.2.9 Manajemen Risiko SI/TI

Menurut Kaye (2011), manajemen risiko diartikan sebagai identifikasi, analisis dan kontrol risiko yang dapat mengancam operasi, aset dan tanggung jawab organisasi. Manajemen risiko ini memiliki tugas tersendiri yaitu mengelola risiko suatu proyek. Tujuan dari dikelolanya risiko tersebut adalah untuk menjaga hubungan ke tingkat yang dapat diterima dengan cara

yang hemat biaya [18]. Jadi, manajemen risiko SI/TI merupakan proses pengidentifikasian, penanganan dan pemantauan terhadap ancaman atau risiko yang bisa terjadi terhadap aset teknologi informasi yang berkaitan langsung dengan bisnis perusahaan.

Pada umumnya manajemen risiko SI/TI akan diikuti degan penentuan prioritas risiko yang dapat memberikan dampak kerugian bagi organisasi atau perusahaan, serta prioritas dalam penanganannya. Langkah – langkah yang dapat dilakukan oleh organisasi atau perusahaa dalam penanganan risiko adalah sebagai berikut :

a. Accept
Manajemen memutuskan untuk menerima risiko jika besarnya dampak dan tingkat kecenderungan masih dalam batas toleransi organisasi.

b. Avoid
Organisasi memutuskan untuk tidak melakukan suatu aktivitas atau memilih alternatif aktivitas lain yang menghasilkan output yang sama untuk menghindari terjadinya risiko.

c. Mitigate
Organisasi memutuskan untuk mengurangi dampak maupun kemungkinan terjadinya risiko.

d. Transfer
Organisasi memutuskan untuk mengalihkan seluruh atau sebagian tanggun jawab pelaksanaan suatu proses kepada pihak ketiga.

2.2.10FMEA (Failure Mode and Effects Analysis)

FMEA merupakan suatu teknik yang digunakan untuk mengidentifikasi, memprioritaskan, dan menghilangkan

kegagalan yang berpotensi dari sistem, desain atau proses sebelum mereka mencapai pelanggan (Omdahl, 1988). Dengan kata lain, FMEA adalah sebuah prosedur yang terstruktur dalam mengidentifikasi dan mencegah mode kegagalan (*failure mode*) sebanyak mungkin. Yang dimaksud dengan mode kegagalan adalah segala sesuatu yang termasuk dalam kecacatan atau kegagalan dalam desain, kondisi diluar batas spesifikasi atau standar yang telah ditetapkan maupun perubahan pada produk yang menyebabkan terganggunya fungsi dari produk itu sendiri. FMEA memiliki beberapa tahapan, yaitu :

1. Mengidentifikasi komponen serta fungsi yang terkait
2. Mengidentifikasi mode kegagalan *(failure modes)* yang paling potensial
3. Mengidentifikasi dampak dari mode kegagalan *(failure mode)*
4. Mengidentifikasi penyebab dari kegagalan
5. Menentukan nilai keparahan *(severity)* dari kegagalan
6. Menentukan nilai frekuensi sering terjadinya kegagalan *(occurrence)*
7. Mengidentifikasi kontrol yang diperlukan
8. Menentukan nilai keefektifan kontrol yang sedang berjalan *(detection)*
9. Melakukan perhitungan nilai RPN *(Risk Priority Number)*
10. Menentukan tindakan untuk mengurangi kegagalan.

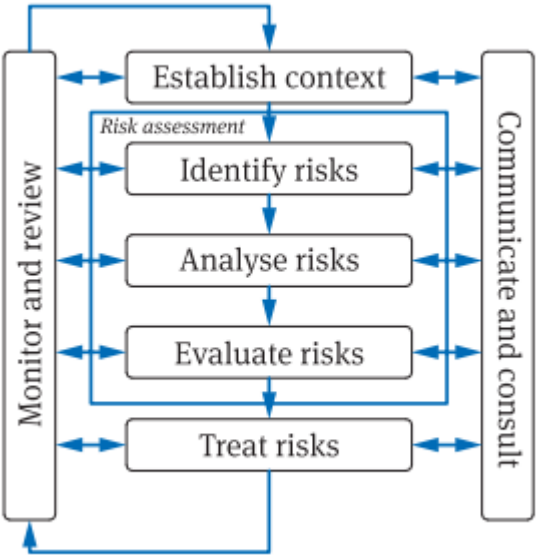
2.2.11ISO 31000 Risk Management

ISO 31000 merupakan salah satu standar yang dapat digunakan dalam melakukan manajemen risiko. ISO 31000 berisikan prinsip – prinsip dan pedoman umum dalam melakukan manajemen risiko sehingga standar ini dapat digunakan atau diterapkan oleh berbagai kalangan.

Meskipun ISO 31000 menyediakan pedoman yang bersifat umum, namun hal ini tidak bertujuan untuk mengharuskan

keseragaman dalam manajemen risiko pada organisasi atau perusahaan. Dalam mendesain dan juga mengimplementasikan rencana manajemen risiko dan kerangka kerjanya perlu mempertimbangkan hal – hal tertentu seperti tujuan tertentu, konteks, struktur, operasi, proses, produk, jasa atau aset dan praktik tertentu yang dipergunakan [19].

Proses pengelolaan risiko menurut ISO 31000 harusnya menjadi sebuah bagian yang terintegrasi dan melekat dalam budaya serta praktik manajemen organisasi. Dalam *Risk Management Process* ISO 31000, *Risk Asesment* menjadi bagian yang paling penting serta fundamental dalam proses pengelolaan risiko. Gambaran Risk Management Process ISO 31000 dapat dilihat pada Gambar 2.2 di bawah ini.



Gambar 2.2 ***The ISO 31000:2009 Risk Management Process***

Pada penelitian kali ini, identifikasi risiko akan dilakukan dengan mengikuti konsep *Risk Assesment* dari *Risk Management Process* ISO 31000. Untuk lebih detailnya proses yang ada pada asesmen risiko adalah sebagai berikut :

1. Identifikasi risiko : proses identifikasi risiko terhadap aset yang ada di ruang server milik STIE Perbanas Surabaya. Dengan mengidentifikasi ancaman dan juga kerentanan aset yang ada di ruang server terlebih dahulu, akan mempermudah dalam melakukan identifikasi risiko. Proses ini akan menghasilkan sebuah *risk register*.

2. Analisis risiko : analisis risiko akan dilakukan dengan menggunakan metode FMEA, dengan menentukan nilai dari tingkat keparahan (*severity*), frekuensi kejadian (*occurence*), dan juga keefektifan dari kontrol (*detection*) serta dampak yang ditimbulkan terlebih dahulu. Dalam proses penilaian untuk setiap risiko nya akan didiskusikan dengan pihak Bagian TIK STIE Perbanas Surabaya untuk menghasilkan penilaian yang lebih akurat dan sesuai dengan harapan dari pihak STIE Perbanas Surabaya. Proses ini akan menghasilkan daftar risiko berserta penilaiannya.

3. Evaluasi risiko : untuk evaluasi risiko akan dilakukan dengan mempertimbangkan nilai RPN (*Risk Priority Number*). Dari hasil penilaian tingkat keparahan (severity), frekuensi kejadian (occurence), dan juga keefektifan dari kontrol (detection) kemudian dicari nilai RPN untuk setiap risikonya. Selanjutnya hasil penilaian RPN dipetakan sesuai dengan level RPN menurut FMEA seperti tabel 2.3 di bawah ini.

Tabel 2.3 Klasifikasi Level Risiko Berdasarkan RPN Menurut FMEA

CLASS OF RPN CATEGORISM	
RPN Calculation	***Level***
< 20	*Very Low*
< 80	*Low*
< 120	*Medium*
< 200	*High*
> 200	*Very High*

Selanjutnya risiko dipetakan ke dalam *Control Objective* dari ISO 27002:2013 klausul keamanan fisik dan lingkungan. Sehingga proses ini akan menghasilkan risiko yang sudah dipetakan ke dalam kontrol objektif ISO 27002:2013 untuk klausul keamanan fisik dan lingkungan.

2.2.12 *ISO/IEC 27002:2013* Klausul Keamanan Fisik dan Lingkungan

ISO/IEC 27002 merupakan salah satu standar untuk keamanan informasi dimana standar ini berisikan panduan yang menjelaskan contoh – contoh penerapan keamanan informasi dengan menggunakan bentuk kontrol tertentu agar dapat mencapai tujuan atau sasaran dari kontrol yang telah ditetapkan sebelumnya. Bentuk kontrol ISO/IEC 27002 seluruhnya menyangkut 11 area pengamanan sebagaimana ditetapkan dalam ISO/IEC 27001 dan salah satu kontrol tersebut adalah Keamanan Fisik dan Lingkungan (*Physical and Environmental Security*). Pada tabel 2.4 berikut ini merupakan daftar dari *Controls* dan *Objectives* ISO 27002:2013 terkait dengan Kemanan Fisik dan Lingkungan (*Physical and Environmental Security*) [20].

Tabel 2.4 Control Objective ISO 27002:2013 Klausul Keamanan Fisik dan Lingkungan

Point Utama	*Control Objective*	Penjelasan
11.1 Secure area		Untuk mencegah akses secara fisik oleh pihak tidak berwenang, kerusakan dan interferensi terhadap lokasi serta informasi dari organisasi.
	11.1.1 Physical security perimeter	Perimeter keamanan (batasan seperti dinding, pintu masuk yang dikendalikan dengan kartu akses 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 bahwa hanya personel yang berwenang yang diperbolehkan

Point Utama	*Control Objective*	Penjelasan
		untuk mengaksesnya.
	11.1.3 Securing office, rooms and facilities	Keamanan fisik untuk kantor, ruangan serta fasilitas harus dirancang dan diimplementasikan .
	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 diimplementasikan .
	11.1.5 Working in secure areas	Perlindungan fisik dan pedoman kerja dalam area yang aman harus dirancang dan diimplementasikan .
	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,

Point Utama	*Control Objective*	Penjelasan
		dipisahkan dari fasilitas pengolahan informasi untuk mencegah akses tidak berwenang.
11.2 Equipment security		Untuk mencegah kehilangan, kerusakan, pencurian atau gangguan aset dan interupsi terhadap kegiatan organisasi
	11.2.1 Equipment sitting 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 serta telekomunikasi yang membawa data atau jasa informasi pendukung harus

Point Utama	*Control Objective*	Penjelasan
		dilindungi dari 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 pihak 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 Secure disposal or re-use of equipment	Seluruh item atau peralatan yang memuat media penyimpanan harus diperiksa untuk memastikan bahwa setiap data sensitif dan perangkat lunak berlisensi telah dihapus atau ditimpa (*overwritten*) secara aman sebelum dibuang.

Point Utama	*Control Objective*	Penjelasan
	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.

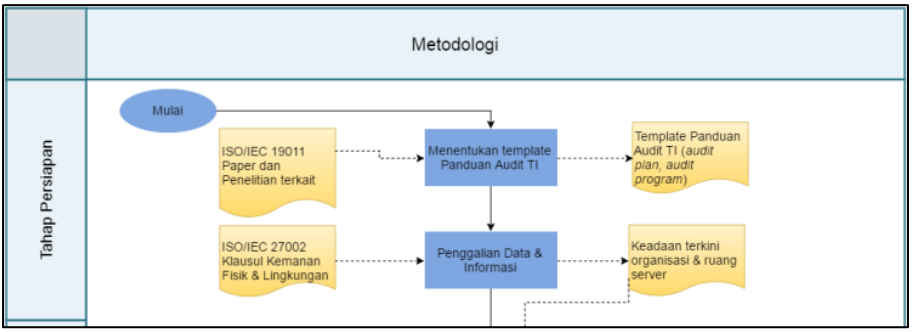
Halaman ini sengaja dikosongkan

BAB III
METODOLOGI PENELITIAN

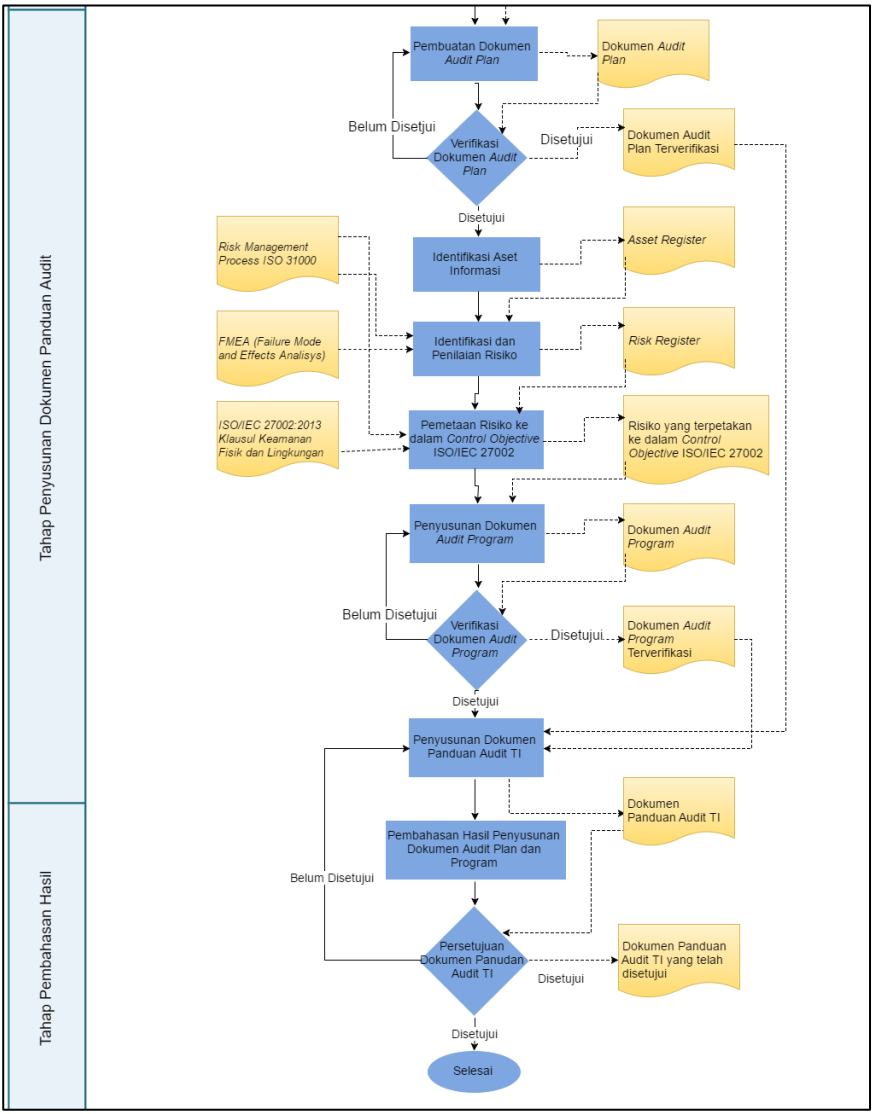
Pada bagian ini akan dijelaskan mengenai metodologi dalam penyusunan tugas akhir sehingga langkah-langkah pengerjaan menjadi lebih sistematis dan terorganisir dengan rapi.

3.1 Gambar Metodologi Penelitian

Berikut ini merupakan gambar metodologi penelitian yang akan digunakan.



Gambar 3.1 Metodologi Penelitian Tahap 1



Gambar 3.2 Metodologi Penelitian Tahap 2 dan 3

3.2 Tahapan Pelaksanaan Penelitian

Dengan mengacu pada ISO/IEC 19011, pada pengerjaan tugas akhir ini akan melewati beberapa tahapan yaitu tahap persiapan, tahap penyusunan dokumen panduan audit, dan juga tahap pembahasan hasil. Pada bab ini akan dijelaskan secara lebih mendetail terkait masing – masing tahapan tersebut.

3.2.1 Tahap Persiapan

Tahap yang paling awal adalah tahap persiapan. Tahapan ini dilaksanakan untuk mengumpulkan berbagai macam informasi yang akan digunakan dalam penyusunan dokumen panduan audit teknologi informasi. Adapaun aktivitas atau proses pada tahap persiapan ini adalah sebagai berikut :

1) Menentukan Template Panduan Audit
   Dalam menentukan template panduan audit yang akan digunakan, terdapat beberapa input diantaranya ISO/IEC 19011 yang dapat dijadikan acuan untuk menentukan konten dari sebuah *audit plan* dan *audit program* (panduan audit), serta paper atau penelitian lain yang menghasilkan dokumen panduan audit.

2) Penggalian Data dan Informasi
   Proses ini adalah proses kedua pada tahap persiapan. Proses ini dilakukan untuk memperoleh data dan informasi mengenai keadaan terkini dari organisasi termasuk juga ruang server milik STIE Perbanas Surabaya. Selain itu, penggalian data juga dilakukan untuk memperoleh informasi – informasi lain yang diperlukan dalam penyusunan dokumen *audit plan* serta *audit program* pada proses selanjutnya. Pengumpulan data dan informasi ini dilakukan dengan dua cara yaitu ;

   a. Wawancara
      Proses wawancara dilakukan secara langsung kepada Wakil Ketua 1 STIE Perbanas Surabaya (Pembantu Ketua Bidang Akademik) dan Ketua SIE TIK

(Manajemen Jaringan dan Technical Support). Dengan melakukan wawancara ini diharapkan penulis dapat memperoleh kondisi terkini dari SIE TIK STIE Perbanas Surabaya terutama yang berkaitan dengan keamanan fisik dan lingkungan dari ruang server yang dimiliki.

b. Observasi
Observasi dilakukan dengan mengumpulkan data dan informasi melalui pengamatan secara langsung untuk suatu objek tertentu pada periode atau waktu tertentu. Pada penelitian ini, observasi dilakukan dengan melakukan pengamatan secara langsung terhadap manajemen keamanan informasi yang ada di STIE Perbanas Surabaya.

3.2.2 Tahap Penyusunan Dokumen Panduan Audit

Tahap penyusunan dokumen panduan audit ini merupakan tahapan kedua, dimana pada tahapan ini terdapat beberapa proses yaitu :

1) Pembuatan Dokumen *Audit Plan*
Pembuatan dokumen *audit plan* merupakan proses yang pertama pada tahapan ini. Template yang sudah ditentukan pada tahap persiapan akan digunakan pada proses ini. Penulis akan mulai menyusun dokumen *audit plan* dengan menggunakan data dan informasi terkait kondisi terkini dari organisasi yang didapat dari proses penggalian data dan informasi pada tahap awal serta ditambahkan dengan informasi mengenai proses audit dari ISO 19011:2013.
Secara umum, dokumen *audit plan* akan berisikan beberapa hal yaitu :

   a. Informasi umum yaitu tujuan, ruang lingkup, referensi dokumen yang digunakan, singkatan, dan kontak *auditor* serta *auditee*.
   b. Proses audit yang berisikan tipe audit internal, subjek, peran dan tanggung jawab auditor, metode audit, serta jadwal pelaksanaan audit.

Berikut ini adalah aktivitas yang merupakan sub proses dalam pembuatan dokumen *audit plan* :

a. Menentukan ruang lingkup audit
   Ruang lingkup audit yang akan dilakukan dapat ditentukan dari hasil penggalian data dan informasi pada tahap persiapaan.
b. Menentukan tipe dan metode audit
   Pada proses ini akan ditentukan tipe audit internal serta metode yang akan digunakan selama proses audit. Hal ini dilakukan dengan mengkaji dari dokumen pendukung seperti ISO/IEC 19011 yang merupakan standar untuk audit.
c. Mengidentifikasi aktivitas audit
   Dengan mengacu pada proses audit yang dijelaskan dalam ISO/IEC 19011, semua aktivitas yang akan dilakukan selama proses audit akan diidentifikasi pada proses ini mulai dari tahap persiapan hingga penutupan. Dari proses ini akan didapatkan daftar aktivitas yang akan dilakukan.
d. Membuat jadwal kegiatan
   Dari daftar aktivitas yang sudah berhasil diidentifikasi, selanjutnya akan dibuatkan penjadwalannya. Penjadwalan ini meliputi durasi untuk setiap aktivitas, dan waktu mulai serta berakhirnya setiap aktivitas. Selain itu, pada proses ini juga akan menghasilkan sebuah *Work Breakdown Structure* (WBS).
e. Mengalokasikan sumber daya
   Untuk mengalokasikan sumber daya yang dapat digunakan dalam peroses audit, akan dilakukan wawancara dengan pihak STIE Perbanas Surabaya sehingga rencana aktivitas yang sudah dibuat dapat disesuaikan dengan ketersediaan sumber daya yang ada.

Dalam penyusunan dokumen *audit plan* ini, penulis melakukan wawancara dengan pihak STIE Perbanas Surabaya untuk memperoleh informasi terkait dengan

kontak auditor dan auditee serta memastikan berapa lama audit akan berlangsung. Penulis akan menggunakan ISO 19011 sebagai acuan dalam pengerjaan bagian lain seperti peran dan tanggung jawab, serta metode dan juga tipe audit yang digunakan. Hasil atau output dari proses ini adalah sebuah dokumen *audit plan*.

2) Verifikasi Dokumen *Audit Plan*
Proses ini bertujuan untuk mengetahui apakah setiap poin yang ada pada dokumen audit plan sudah benar dan sesuai. Dokumen audit plan akan diserahkan kepada pihak STIE Perbanas Surabaya untuk diverifikasi. Verifikasi yang dilakukan dengan pihak STIE Perbanas Surabaya hanya yang berkaitan dengan semua informasi yang diminta dari pihak STIE Perbanas Surabaya. Selebihnya akan dilakukan peninjauan ulang dengan dokumen lain yang terkait. Apabila pada proses ini masih terdapat kesalahan, maka penulis akan melakukan perbaikan terhadap dokumen dan mengulang proses pembuatan dokumen *audit plan* hingga dokumen audit plan dapat diterima dan disetujui oleh pihak STIE Perbanas Surabaya. Hasil dari proses ini adalah dokumen *Audit Plan* yang sudah diverifikasi.

3) Identifikasi Aset Informasi
Identifikasi aset informasi merupakan proses pengidentifikasian aset informasi dan teknologi informasi serta semua infrastruktur yang dimiliki oleh STIE Perbanas Surabaya yang disimpan dalam ruang servernya. Proses ini dilakukan dengan cara observasi langsung dan wawancara dengan pihak terkait yaitu Kepala Bagian TIK STIE Perbanas Surabaya untuk mendapatkan informasi terkait aset apa sajakah yang dimiliki pada ruang server. Pada tahap ini akan diperoleh data dan informasi mengenai semua aset yang dimiliki dan disimpan pada sebuah ruang server yang kemudian

akan ditulis dalam bentuk *asset register* yang akan digunaakan untuk proses selanjutnya.

4) Identifikasi dan Penilaian Risiko
   Pada proses ini, penulis akan melakukan identifikasi risiko TI terhadap aset yang dimiliki dengan menggunakan *ouput* atau hasil dari proses sebelumnya yaitu *asset register*. Dengan mengacu pada *Risk Management Process* ISO 31000, selanjutnya, risiko yang sudah berhasil diidentifikasi akan dinilai dengan menggunakan metode FMEA dengan mempertimbangkan nilai *severity, occurrence, detection*. Proses ini akan menghasilkan sebuaah *risk register* untuk setiap aset yang ada. Penilaian terhadap risiko yang sudah teridentifikasi akan dibicarakan dengan pihak STIE Perbanas Surabaya untuk menghasilkan *risk register* yang lebih tepat dan sesuai.

5) Pemetaan Risiko ke dalam *Control Objective* ISO/IEC 27002:2013 Klausul Keamanan Fisik dan Lingkungan
   Pemetaan risiko merupakan proses dimana *risk register* yang sudah tepat dan sesuai akan dipetakan ke dalam *control objective* yang ada pada ISO/IEC 27002:2013 terkait dengan keamanan fisik dan lingkungan. Pada proses ini akan menghasilkan daftar risiko yang sudah dipetakaan ke dalam *control objective* ISO/IEC 27002:2013 terkait dengan keamanan fisik dan lingkungan. Semua *control objective* yang sudah berhasil dipetakan akan disesuaikan dengan kontrol yang sudah diterapkan oleh pihak STIE Perbanas Surabaya untuk keamanan fisik dan lingkungan ruang server yang dapat memenuhi *control objective* sesuai dengan hasil pemetaannya. Sehingga *output* atau hasil dari proses ini adalah risiko dan kontrolnya yang sudah terpetakan ke dalam *Control Objective* ISO/IEC 27002:2013 klausul Keamanan Fisik dan Lingkungan.
6) Penyusunan Dokumen *Audit Program*

Penyusunan dokumen *audit program* merupakan proses selanjutnya dari tahapan penyusunan dokumen panduan audit. *Template* dokumen *audit program* yang sudah ditentukan pada tahap persiapan akan digunakan pada proses ini. Penulis akan mulai menyusun dokumen panduan audit TI dengan mengacu pada dokumen *audit plan* serta risiko dan kontrolnya yang sudah dipetakan ke dalam *control objective* ISO/IEC 27002:2013 terkait dengan keamanan fisik dan lingkungan untuk ruang server STIE Perbanas Surabaya.

Dokumen *Audit Program* berisikan tujuan dari dokumen audit program, kendali tujuan yang digunakan, prosedur program audit, serta dokumen kerja audit. Pada bagian prosedur program audit atau *checklist* audit, berisikan prosedur untuk setiap kontrol dan daftar cek yang diperlukan. Selain itu akan terdapat juga panduan untuk penggunaan dokumen *audit program* yang berisikan tata cara penggunaan dari prosedur audit.

Berikut ini adalah aktivitas yang dilakukan dalam penyusunan dokumen *audit program* secara lebih spesifik :

a) Pembuatan Informasi Umum
   Bagian informasi umum ini berisikan tujuan, analisis risiko, *control objective,* acuan serta proses audit. Analisis risiko yang dimaksud pada bagian ini adalah hasil identifikasi risiko terkait dengan keamanan fisik dan lingkungan untuk ruang server milik STIE Perbanas Surabaya yang akan ditampilkan dalam bentuk tabel. *Control objective* akan didapatkan dari risiko dengan nilai RPN tinggi atau yang termasuk dalam kategori *High.* Acuan yang dimaksud adalah dokumen – dokumen lain yang dapat digunakan dalam penyusunan prosedur program audit.
b) Pembuatan Perangkat Audit

Bagian ini terdiri dari Prosedur Audit Pemeriksaan yang berisikan daftar *control objective* yang harus diperiksa dan akan ditampilkan dalam bentuk tabel. Daftar *control objective* ini didapatkan dari tabel hasil identifikasi dan penilaian risiko yang memiliki nilai RPN dalam kategori *Very High*, *High*, dan *Medium*. Kemudian, dari daftar *control objective* tersebut akan dibuatkan daftar cek audit atau *audit checklist* untuk setiap prosedur pemeriksaan. *Checklist* ini akan berisikan bagaimana cara dalam melakukan prosedur pemeriksaan, status dari komponen yang diperiksa (sesuai, tidak sesuai, dan parsial), serta justifikasi terkait dengan pemberian status komponen yang diperiksa. Selanjutnya, pada proses ini juga dilakukan pembuatan formulir tindak lanjut temuan audit dimana formulir ini akan berisikan rangkuman hasil temuan audit, rekomendasi perbaikan, penanggung jawab, serta batas waktu penyelesaian perbaikan yang dilakukan.

c) Pembuatan Panduan Penggunaan Audit Program
Secara umum, bagian ini akan menjelaskan bagaimana tata cara penggunaan setiap dokumen yang menjadi bagian dan ada pada audit program termasuk formulir serta *audit checklist.*

7) Verifikasi Dokumen *Audit Program*
Verifikasi dokumen *audit program* merupakan proses dimana penulis akan melakukan verifikasi dari pihak STIE Perbanas Surabaya serta melakukan pengkajian ulang yang mengacu pada standar yang digunakan yaitu ISO/IEC 27002:2013 terkait dengan *audit program* yang telah dibuat. Verifikasi dilakukan dengan pengecekan terhadap prosedur audit yang ada pada dokumen audit program untuk memastikan kesesuaiannya dengan standar ISO/IEC 27002:2013.
8) Penyusunan Dokumen Panduan Audit
Pada tahap ini, dokumen *audit plan* dan juga *audit program* yang sudah diverifikasi oleh pihak STIE

Perbanas Surabaya akan dijadikan dalam satu bentuk buku atau dokumen. Ouput atau hasil dari proses ini adalah sebuah Dokumen Panduan Audit TI.

3.2.3 Tahap Hasil dan Pembahasan

Secara garis besar, tahapan ini berisikan pembahasan isi dokumen *audit plan* dan *audit program* serta proses validasi atau persetujuan dokumen panduan audit TI yang sudah dibuat dari pihak STIE Perbanas Surabaya.

1) Pembahasan Hasil Penyusunan Dokumen *Audit Plan* dan *Audit Program*
   Tahap pembahasan isi dari dokumen Audit Plan serta Audit Program yang telah selesai dibuat oleh penulis
2) Persetujuan Dokumen Panduan Audit TI
   Merupakan proses terakhir yang dilakukan. Pada proses ini penulis melakukan persetujuan dengan pihak STIE Perbanas Surabaya terhadap dokumen panduan audit TI yang telah dibuat. Apabila pihak STIE Perbanas Surabaya merasa bahwa dokumen panduan audit TI masih ada yang kurang sesuai, maka akan dilakukan perbaikan dengan mengulang ke proses penyusuanan dokumen panduan audit. Jika memang sudah sesaui, Dokumen audit plan dan audit program yang tersusun dalam Dokumen Panduan Audit TI akan ditandatangani sehingga dokumen tersebut siap untuk digunakan.

BAB IV
PERANCANGAN

Bagian ini akan menjelaskan mengenai tahap persiapan dari penelitian tugas akhir. Pada tahap persiapan ini terdapat dua proses utama yaitu penentuan template dan juga penggalian data serta informasi.

4.1 Penentuan Template

Template merupakan sebuah model atau standar yang dapat dijadikan sebagai sebuah pembanding. Dalam penelitian ini, template yang dimaksud merupakan standar dari isi sebuah dokumen panduan audit (*audit plan & audit program*) yang akan dibuat. Salah satu standar yang dapat digunakan untuk menentukan apa saja isi dari sebuah panduan audit adalah ISO 19011. Pada standar ini dijelaskan mengenai hal – hal yang harus terdapat pada sebuah *audit plan* yaitu :

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

Selain berdasarkan standar ISO 19011, dalam pembuatan dan penyusunan sebuah *audit plan* juga dapat mengacu pada PMBOK yang merupakan standar untuk sebuah *project plan*. Standar ini akan sangat membantu dalam penyusunan *audit plan* terutama dalam pengidentifikasian aktivitas dan pengalokasian waktu serta suberdaya selama proses audit yang direncanakan.

Pada ISO 19011 juga sudah dijelaskan mengenai cakupan dari sebuah program audit dimana audit program harus berisikan hal – hal berikut :

a. Tujuan untuk program audit dan audit individu.
b. Prosedur program audit.
c. Kriteria audit.
d. Metode audit.
e. Pemilihan tim audit.
f. Sumber daya yang diperlukan, termasuk perjalanan dan akomodasi.
g. Proses untuk menangani kerahasiaan, keamanan informasi, kesehatan dan keselamatan, dan hal-hal lain yang sejenis.

Selain hal – hal yang sudah disebutkan, dalam penyusunan dokumen panduan audit ini, peneliti juga akan menggunkan hasil penelitian atau tugas akhir dengan topik yang sama sebagai acuan lainnya. Salah satu hasil penelitian yang akan digunakan adalah hasil penelitian dari Stephen (2015), dengan judul "*Pembuatan Panduan Audit Kemanan Fisik dan Lingkungan Teknologi Informasi Berbasis Risiko Berdasarkan ISO/IEC 27002:2013 Pada Direktorat Sistem Informasi Universitas Airlangga"*. Sehingga audit program pada penelitian ini akan berisikan hal – hal berikut :

- Tujuan serta ruang lingkup audit,
- Best practice dan kendali tujuan,
- Dokumen Prosedur audit,
- Dokumen atau formulir kerja audit.

4.2 Persiapan Penggalian Data

Proses selanjutnya pada tahapan persiapan adalah perispan penggalian data dan informasi. Terdapat beberapa metode yang dapat digunakan dalam proses ini. Dalam sebuah artikel karya Said (2015), mengatakan bahwa pada sebuah penelitian terdapat

5 teknik dalam pengumpulan data diantaranya adalah wawancara, observasi, kuesionair, tes, dan dokumen.

4.2.1 Teknik Pengumpulan Data

Pada penelitian ini, metode atau teknik yang akan digunakan dalam pengumpulan data dan informasi diantaranya adalah wawancara, observasi, dan dokumen. Proses wawancara akan lebih banyak dilakukan dengan bagian TIK STIE Perbanas Surabaya yang memiliki wewenang serta tanggung jawab lebih terhadap teknologi informasi milik STIE Perbanas Surabaya. Adapun narasumber yang digunakan adalah kepala Bagian TIK STIE Perbanas Surabaya. Proses wawancara ini dilakukan untuk menggali informasi mengenai beberapa hal seperti aset berupa teknologi informasi yang dimiliki, praktik keamanan terkini terhadap ruang server, risiko yang dimiliki, serta proses audit yang sudah pernah dilakukan. Metode observasi dan dokumen dilakukan untuk memastikan kebenaran hasil wawancara yang sudah didapatkan seperti dengan menyesuaikan daftar aset yang dimiliki dengan hasil wawancara yang didapat, serta melihat secara langsung praktik keamanan terhadap ruang server.

4.2.2 Informasi yang Diperlukan

Dari metode atau teknik pengumpulan data dan informasi yang sudah dilakukan sebelumnya, berikut ini adalah pemaparan secara lebih detail mengenai data yang ingin diperoleh selama proses ini berlangsung :

1. Daftar aset teknologi inforamsi yang ada pada ruang server.
2. Kontak SDM yang dapat digunakan sebagai auditor dan auditee.
3. Praktik keamanan atau manajemen keamanan terkini pada ruang server.
4. Audit internal yang pernah dilakukan terhadap bagian TIK STIE Perbanas Surabaya.
5. Waktu pelaksanaan audit internal yang pernah dilakukan.

6. Ketersediaan dokumen prosedur atau kebijakan yang terkait dengan perawatan, pemeliharaan, pengadaan ataupun pemusnahan aset TI yang dimiliki.

4.3 Pengolahan Data

Dalam pengolahan data dan informasi yang telah berhasil diperoleh, terdapat dua metode yang akan digunakan. Metode pertama bertujuan untuk memudahkan penulis dalam melakukan analisis terhadap hasil wawancara yang didapatkan yaitu dengaan melakukan penulisan ulang tekait hasil wawancara yang diperoleh dengan bantuan *tools* berupa *Microsoft Word.*

Selanjutnya barulah dilakukan pengolahan data dengan melakuakan identifikasi risiko untuk setiap aset yang dimiliki. Kemudian akan dilakukan penilaian terhadap risiko dengan menggunakan metode FMEA yang memiliki aspek penilaian risiko berdasarkan *Saverity, Occurance,* serta *Detection*. Berikut adalah kriteria perhitungan untuk masing – masing nilai.

a. Penentuan Nilai Dampak (*Saverity* = S)
   Pengukuran nilai dari dampak dapat dilihat dari seberapa sering atau intensitas suatu kejadian maupun gangguan yang dapat mempengaruhi aspek -aspek penting. Dalam menentukan penilaian dari tingkat dampak, perlu sebuah parameter untuk setiap nilainya. Berikut ini merupakan penjelasan dari masing – masing nilai tingkat dampak (*Saverity*).

Tabel 4.1 Tabel Penilaian Saverity

Peringkat	Efek	Efek dari severity
10	Berbahaya; tanpa peringatan	Menyebabkan proses bisnis terhenti untuk waktu lama > 1 minggu
9	Berbahaya; dengan peringatan	Menyebabkan proses bisnis terhenti untuk waktu cukup lama > 1 hari
8	Sangat Tinggi *(very high)*	Menyebabkan proses bisnis terhenti sebentar < 1 hari
7	Tinggi *(high)*	Menghambat berjalannya proses bisnis
6	Sedang *(moderate)*	Menyebabkan tidak berfungsinya layanan seperti semestinya
5	Rendah *(low)*	Menimbulkan komplain
4	Sangat Rendah *(very low)*	Menyebabkan gangguan yang cukup berpengaruh
3	Sedikit *(minor)*	Menyebabkan sedikit gangguan
2	Sangat sedikit *(very minor)*	Tidak diperhatikan, berpengaruh minor terhadap kinerja
1	Tidak ada *(none)*	Tidak diperhatikan maupun mempengaruhi kinerja

b. Penentuan Nilai Kemungkinan (*Occurrence* = O)
Pengukuran nilai kemungkinan merupakan pengukuran terhadap kemungkinan bahwa penyebab dari kegagalan akan terjadi dan mengakibatkan kegagalan suatu proses. Nilai kemungkinan merupakan pengukuran terhadap

tingkat frekuensi terjadinya suatu masalah atau gangguan yang dapat mengakibatkan kegagalan. Berikut ini merupakan penjelasan dari setiap nilai *Occurrence.*

Tabel 4.2 Tabel Penilaian Occurrence

Peringkat	Efek	Kemungkinan terjadi
10	*Sangat tinggi* – kegagalan hampir tak terelakan	> 1 kali / hari
9		1 kali / hari
8	*Tinggi* – Kegagalan Sering terjadi	1 kali / 3-4 hari
7	*Sedang* – Cukup sering terjadi	1 kali / minggu
6		1 kali / 2 minggu
5		1 kali / bulan
4	*Rendah* – cukup jarang terjadi	1 kali / 3 bulan
3		1 kali / 6 bulan
2	*Sangat Rendah* – Jarang terjadi	1 kali / tahun
1	*Hampir tidak mungkin* :Hampir tidak mungkin terjadi	1 kali / beberapa tahun

c. Penentuan Nilai Deteksi (*Detection* = D)
Pengukuran nilai deteksi adalah penilaian terhadap kemampuan dari organisasi dalam melakukan kontrol dan mengendalikan suatu gangguan yang dapat mengakibatkan kegagalan. Berikut ini adalah penjelasan dari setiap nilai *Detection*.

Tabel 4.3 Tabel Penilaian Detection

Peringkat	Efek	Deteksi
10	*Hampir tidak mungkin*	Potensi penyebab tidak terdeteksi atau tidak dapat dikontrol
9	*Sangat sulit*	Sangat sulit untuk mendeteksi risiko , sangat sulit dikendalikan
8	*Sulit*	Sulit dideteksi, sulit dikendalikan
7	*Cukup sulit*	Cukup sulit dideteksi, cukup sulit dikendalikan
6	*Normal*	Dapat dideteksi dengan usaha ekstra, dapat dikendalikan dengan usaha extra

Peringkat	Efek	Deteksi
5	*Sedang*	Dapat dideteksi, dapat dikendalikan
4	*Cukup mudah*	Cukup mudah dideteksi, cukup mudah dikendalikan
3	*Mudah*	Mudah dideteksi, mudah dikendalikan
2	*Sangat mudah*	Sangat mudah dideteksi, sangat mudah dikendalikan
1	*Hampir pasti*	Terlihat jelas, sangat mudah pengendaliannya

4.4 Pendekatan Analisis

Setelah pelaksanaan proses pengumpulan data, selanjutnya dilakukanlah proses analisis terhadap data. Dalam melakukan analisis terhadap data, terdapat beberapa pendekatan yang dapat digunakan, yaitu :

1. **Analisis menggunakan pendekatan konseptual**
   Analisis pendekatan konseptual dilakukan dengan menganalisa tugas pokok serta fungsi yang ada pada bagian TIK STIE Perbanas Surabaya terkait dengan tanggung jawab dalam pengelolaan ruang server serta

praktik keamanan secara fisik dan lingkungan yang diterapkan pada ruang server guna mengetahui kondisi terkini dan kemudian dipetakan ke dalam standar yang digunakan yaitu ISO/IEC 27002:2013.

2. Analisis menggunakan pendekatan standar

a. ISO/IEC 27002:2013 – Keamanan Fisik dan Lingkungan

   Analisis dengan standar ISO/IEC 27002:2013 pada klausul keamanan fisik dan lingkungan digunakan untuk mengetahui praktik keamanan terhadap ruang server yang sesuai dengan standar.

b. PMBOK – *Project Plan*

   Analisis dengan menggunakan PMBOK pada proses *Project Plan* digunakan dalam menganalisa hal – hal yang diperlukan untuk penyusunan dokumen *audit plan* seperti penyususnan aktivitas, jadwal, sumber daya dan yang lainnya.

Halaman ini sengaja dikosongkan

BAB V
IMPLEMENTASI

Pada bab ini akan dijelaskan terkait dengan penerapan atau implementasi dari setiap tahapan dan juga proses dalam metodologi pengerjaan tugas akhir yang dapat berupa waktu pelaksanaan, lampiran terkait yang berisikan catatan tertentu untuk implementasi suatu proses dan juga berupa hasil dari implementasi itu sendiri.

5.1 Penyusunan Dokumen *Audit Plan* Bagian TIK STIE Perbanas Surabaya

Bagian ini berisikan proses penyusunan dari dokumen *audit plan* untuk Bagian TIK STIE Perbanas Surabaya. Sesuai dengan template yang sudah ditentukan pada tahap persiapan, dokumen *audit plan* yang dibuat akan dibagi ke dalam beberapa bagian yaitu bagian Informasi Umum, Proses Audit, dan bagian Evaluasi.
Seluruh isi dokumen yang lebih mendetail dapat dilihat pada buku produk berupa Dokumen *Audit Plan*.

5.1.1 Penyusunan Bagian Informasi Umum

Bagian informasi umum berisikan informasi mengenai audit yang akan dilaksanakan. Selain itu, pada bagian informasi umum juga berisikan tujuan audit plan, ruang lingkup audit plan, gambaran mengenai objek yang di audit, referensi dokumen, serta kontak auditor dan auditee. Berikut ini adalah penjelasan untuk setiap sub bagian dari informasi umum ;

1. Tujuan
   Dalam pembuatannya, tujuan dari *audit plan* diperoleh dari studi literatur yang dilakukan oleh penulis dengan melihat penelitian serupa yang menghasilkan sebuah dokumen *audit plan*.
2. Ruang Lingkup

Pembuatan sub bagian ruang lingkup mengacu dari literatur berupa penelitian yang juga menghasilkan dokumen *audit plan* dengan melakukan beberapa penyesuaian.

3. Gambaran Sistem
   Untuk sub bagian gambaran sistem dibuat berdasarkan atas hasil wawancara yang dilakukan penulis dengan kepala Bagian TIK STIE Perbanas Surabaya yang dapat dilihat pada Lampiran A. Selain itu penulis juga melakukan observasi langsung ke ruang server milik STIE Perbanas Surabaya dengan ditemani oleh kepala Bagian TIK STIE Perbanas Surabaya.
4. Referensi
   Untuk sub bagian referensi dibuat berdasarkan atas hasil wawancara dengan kepala Bagian TIK STIE Perbanas Surabaya terkait dengan ketersediaan dari beberapa dokumen tata kelola untuk pemeliharaan ruang server yang dapat dilihat pada Lampiran A.
5. Akronim dan Singkatan
   Sub bagian ini dibuat dengan mengacu dari dokumen referensi seperti penelitian yang menghasilkan dokumen *audit plan.*
6. Kontak
   Untuk informasi kontak dari auditor dan auditee diperoleh dari hasil penggalian informasi melalui media email dengan bantuan dari kepala Bagian TIK STIE Perbanas Surabaya.

5.1.2 Penyusunan Bagian Proses Audit

Bagian selanjutnya adalah proses audit. Pada bagian ini berisikan informasi terkait dengan apa saja yang akan dan harus dilaksanakan pada saat proses audit berlangsung. Terdapat juga beberapa sub bab diantaranya ; tipe audit internal, subjek audit internal, peran & tanggung jawab, dan metode audit internal yang diperoleh dari studi literature yang dilakukan oleh penulis, serta sub bagian jadwal kegiatan yang diperoleh dari ISO 19011

[13] dan interview dengan Bagian TIK STIE Perbanas Surabaya yang dapat dilihat pada Lampiran A.

Pada sub bagian jadwal kegiatan audit dijelaskan mengenai daftar aktivitas yang harus dilakukan oleh tim audit sehingga proses dari audit dapat berjalan dengan lebih baik dan maksimal. Sesuai dengan ISO 19011 [13], aktivitas audit dibagi ke dalam tiga bagian utama yaitu *preparation, execution*, dan *closing*. Untuk waktu pelaksanaan audit diperoleh dari hasil wawancara dengan pihak Bagian TIK STIE Perbanas Surabaya yang kemudian dikembangkan.

5.1.3 Penyusunan Bagian Evaluasi

Bagian evaluasi pada *audit plan* berisikan informasi mengenai strategi serta *risk assesment* selama proses pelaksanaan audit. Sub bagian strategi berisikan saran dan kiat – kiat yang ditujukan untuk auditor sehingga dalam pelaksanaan proses audit dapat berjalan lebih terstruktur dan terarah. Pembuatan sub bagian ini mengacu dari studi literatur yang dilakukan oleh penulis.

Sedangkan untuk sub bagian *risk assesment* berisikan hasil identifikasi risiko terkait dengan hal – hal yang mungkin bisa terjadi dan menghambat jalannya proses audit. Sub bagian ini bertujuan untuk membantu auditor mempersiapkan diri dalam menghadapi risiko sehingga dapat mengantisipasi ataupun mengelola risiko dengan lebih baik.

5.2 Verifikasi Dokumen *Audit Plan*

Pada bagian ini akan dijelaskan mengenai prsoes verifikasi terhadap dokumen *Audit Plan.* Verifikasi akan dilakukan 2 kali. Pertama, verifikasi akan dilakukan dengan melibatkan pihak Bagian TIK STIE Perbanas Surabaya. Verifikasi ini bertujuan untuk mengetahui apakah inforamsi yang terdapat pada dokumen *Audit Plan* sudah benar, khususnya pada bagian

Informasi Umum. Proses verifikasi dilakukan dengan wawancara langsung dengan pihak STIE Perbanas Surabaya yang sebelumnya sudah diberikan dokumen *Audit Plan* sehingga sudah mengetahui isi dari dokumen. Hasil dari verifikasi yang dilakukan adalah terdapat perubahan pada bagian informasi umum terkait dengan SPI (Satuan Pengawas Internal) dan waktu pelaksanaan audit internal. Hasil wawancara dapat dilihat pada Lampiran A.

Tabel 5.1 Verifikasi Audit Plan dengan Pihak Organisasi

Susunan Dokumen		**Check**	**Keterangan**
Poin	Proses		
1.	Informasi Umum	☑	Perbaikan pada bagian Akronim dan singkatan serta Kontak
2.	Proses Audit	☑	-
3.	Evaluasi	☑	-

Verifikasi kedua dilakukan dengan cara t*raceback* yaitu mencocokkan aktivitas audit yang ada pada dokumen *Audit Plan* dengan proses audit yang ada pada standar ISO 19011. Hasil dari verifikasi kedua dapat dilihat pada Tabel 5.2 berikut.

Tabel 5.2 Verifikasi Daftar Aktivitas Audit Berdasarkan ISO 19011

Daftar Aktivitas		**Standar ISO 19011**		**Check**
Poin	Proses	Poin	Proses	
1.1	Initation	6.2	Initiating the audit	☑
1.2	Planning	6.3	Preparing audit activitis	☑
3.0	Execution	6.4	Conducting the audit activities	☑
4.0	Closing	6.5	Preparing and distributing audit report	☑

5.3 Identifikasi Aset Ruang Server STIE Perbanas Surabaya

Ruang server STIE Perbanas Surabaya merupakan sebuah tempat yang difungsikan sebagai pusat pengolahan seluruh informasi STIE Perbanas Surabaya yang terdiri atas perangkat keras (hardware), perangkat lunak (*software*), database, dan juga fasilitas pendukung lain yang mendukung. Penglelolaan ruang server ini sendiri merupakan tanggung jawab dari Bagian TIK STIE Perbanas Surabaya.

Pada penelitian tugas akhir ini, asset yang dimaksudkan adalah meliputi physical asset yaitu perangkat keras termasuk jaringan serta manusia. Berikut ini merupakan daftar asset pada ruang server STIE Perbanas Surabaya yang diperoleh dari observasi secara langsung dan ditampilkan pada Tabel 5.3.

Tabel 5.3 Daftar Aset Ruang Server STIE Perbanas Surabaya

No.	Kategori Aset	Jenis Aset
1.	Perangkat Keras (*Hardware*)	Server
2.		Monitor
3.		Flash System Detectore
4.		Pendingin Ruangan (AC)
5.		DVR 1
6.		Modem
7.		UPS
8.		CCTV
9.	Jaringan (*Network*)	Router
10.		Telepon Kabel
11		Kabel Fiber Optik
12.		PABX
13.	SDM (*People*)	Pengelola (Staff bagian TIK)

5.4 Analisa dan Penilaian Risiko

Pada bagian ini akan dijelaskan mengenai proses analisa terhadap risiko serta penilaian risiko yang dilakukan

berdasarkan metode FMEA. Penilaian terhadap risiko TI hanya berfokus pada asset TI milik STIE Perbanas Surabaya yang dikategorikan ke dalam 3 kategori yaitu aset berupa perangkat keras (*hardware)*, jarungan (*network*), dan juga Sumber Daya Manusia (*people*). Pemilihan aset TI yang dilakukan pada analisa kali ini berdasarkan atas risiko terhadap aset yang berkaitan dengan keamanan fisik dan lingkungan teknologi informasi yaitu aset fisik. Untuk aset berupa *software* dan aset logis lainnya tidak bergitu berkaitan dengan keamanan fisik dan lingkungan.

5.4.1 Identifikasi Ancaman

Tahap awal pada proses analisa dan penilaian risiko ini adalah identifikasi ancaman terhadap aset TI pada raung server yang dimiliki oleh STIE Perbanas Surabaya. Proses identifikasi ancaman ini dilakukan dengan menggabungkan informasi yang diperoleh ketika observasi langsung dengan studi literatur yang dilakukan oleh penulis. Di bawah ini adalah hasil analisa ancaman yang dapat di lihat pada Tabel 5.4.

Tabel 5.4 Identifikasi Ancaman terhadap Aset

Aset	*Ancaman*
Server	Hilangnya pasokan daya atau listrik
	Voltase listrik yang tidak stabil
	Kesalahan konfigurasi dan perawatan server
	Temperature ruangan server terlalu tinggi
	Kebocoran air AC pada ruang server
	Debu, kotoran, dan korosi pada hardware
Monitor	Proses perawatan tidak dilakukan dengan benar
	Kesalahan dan kelalaian dalam melaksanakan prosedur kerja
Flash System Detector	Proses perawatan aset tidak dilakukan dengan benar
	Debu dan kotoran pada hardware
Modem	Kesalahan konfigurasi modem

Aset	*Ancaman*
	Proses perawatan tidak dilakukan denga benar
	Hilangnya pasokan daya atau listrik
	Kualitas jaringan yang buruk
DVR1	Kesalahan dan kelalaian dalam melaksanakan prosedur kerja
	Hilangnya pasokan daya atau listrik
	Proses perawatan tidak dilakukan dengan benar
Pendingin ruangan (AC)	Proses perawatan aset tidak dilakukan dengan benar
	Hilangnya pasokan daya atau listrik
	Debu dan kotoran pada hardware
UPS	Debu dan kotoran pada hardware
	Proses perawatan aset tidak dilakukan dengan benar
	Kebutuhan daya yang lebih besar dari kapasitas UPS
CCTV	Proses perawatan aset tidak dilakukan dengan benar
Router	Hilangnya pasokan daya atau listrik
	Kesalahan konfigurasi router
	Kualitas jaringan yang kurang bagus
	Proses perawatan tidak dilakukan dengan benar
Telepon Kabel	Proses perawatan aset tidak dilakukan dengan benar
	Kualitas jaringan telepon yang kurang bagus
Kabel Fiber Optik	Kerusakan akibat kurang perlindungan
	Kesalahan penempatan kabel
PABX	Proses perawatan aset tidak dilakukan dengan benar
	Kualitas jaringan telepon yang kurang bagus
Pengelola (Staff)	Penggunaan peralatan tidak sah dalam pelaksanaan prosedur kerja
	Keterbatasan jumlah tenaga kerja

5.4.2 Identifikasi Kerentanan

Kerentanan merupakan suatu kondisi dimana ancaman tidak dapat mengeksploitasi prosedur keamanan, kontrol fisik maupun teknik, ataupun kontrol yang lainnya. Dengan kata lain, kerentanan ini berasal dari aset itu sendiri sehingga akan berpengaruh dalam terjadinya risiko karena memungkinkan ancaman untuk membahayakan aset. Kerentanan akan diidentifikasi berdasarkan aset yang ada pada ruang server dan akan dipergunakan dalam melakukan identifikasi risiko. Berikut ini adalah hasil dari identifikasi kerentanan yang dapat dilihat pada tabel 5.5.

Tabel 5.5 Identifikasi Kerentanan Aset

Aset	*Kerentanan*
Server	Kebutuhan akan daya listrik yang stabil
	RAM mengalami overload
Monitor	Mengalami dead pixel
Flash System Detector	Sensor tidak dapat berfungsi sebagai mana mestinya
Modem	Mengalami overheat
DVR1	Kebutuhan akan daya listrik yang stabil
Pendingin ruangan (AC)	Tidak dapat menghasilkan temperature yang sesuai dengan kebutuhan yang telah ditetapkan
	Mengalami kebocoran akibat kinerja berlebih
UPS	Kapasitas UPS lebih kecil dari power outage
	Baterai UPS tidak bertahan lama
CCTV	Kualitas gambar yang kurang tajam
	Sudut rekam gambar sempit
Router	Jangkauan signal terbatas atau kecil
	Mengalami overheat
Telepon Kabel	Durabilitas alat rendah
	Kabel tetepon mengalami korosi
Kabel Fiber Optik	Kualitas kabel yang mudah rusak atau terputus
	Kabel mengalami korosi

Aset	*Kerentanan*
PABX	Korosi pada hardware
Pengelola (Staff)	Kesadaran akan keamanan yang masih kurang
	Keterbatasan kemampuan staff

5.4.3 Identifikasi Risiko

Risiko yang dimaksudkan pada bagian ini adalah segala kejadian yang kemungkinan bisa terjadi pada suatu hari dan akan memberikan dampak buruk terhadap proses bisnis organisasi. Dari ancaman dan kerentanan yang telah diidentifikasi, selanjutnya dilakukaan identifikasi risiko terhadap aset pada ruang server STIE Perbanas Surabaya, dimana ancaman dan juga kerentanan untuk setiap aset dapat menjadi faktor pembentuk penyebab risiko untuk setiap aset yang ada. Identifikasi risiko yang dilakukan pada bagian ini adalah identifikasi terhadap risiko yang berkaitan dengan keamanan fisik dan lingkungan teknologi informasi, termasuk di dalam nya adalah perangkat pendukung (*supporting uttilities*) yang menunjang kinerja atau ketersediaan perangkat yang ada di ruang server STIE Perbanas Surabaya. Hasil dari identifikasi risiko dapat dilihat pada Tabel 5.6 *Risk Register* berikut ini.

Tabel 5.6 *Risk Register*

ID	Kategori Aset	Nama Aset	Risk ID	Penyebab	Risiko	Dampak Langsung
1	Hardware	Server	R-01	Hilangnya pasokan daya atau listrik	Kerusakan Hardware	Kerusakan pada asset Server down Proses bisnis yang bergantung dengan server terkait terganggu Mengancam keselamatan
			R-02	Temperatur ruangan terlalu tinggi (*Overheat*)		
			R-03	Kesalahan konfigurasi dan perawatan hardware		
			R-04	Bencana alam (petir, gempa bumi, angina kencang)		
2	Hardware	Monitor	R-05	Proses perawatan aset tidak dilakukan dengan benar	Kerusakan Hardware	Kerusakan pada hardware Aktivitas yang bergantung dengan monitor terkait terganggu
			R-06	Kesalahan dan kelalaian dalam melaksanakan prosedur kerja		
3	Hardware	Flash System Detector	R-07	Proses pearawatan aset tidak dilakukan dengan benar	Kerusakan Hardware	Hardware tidak dapat berfungsi

ID	Kategori Aset	Nama Aset	Risk ID	Penyebab	Risiko	Dampak Langsung
4	Hardware	Modem	R-08	Temperatur hardware terlalu tinggi (*overheat*)	Kerusakan Hardware	Jaringan internet terganggu Jaringan menjadi lemot Jaringan tidak tersedia
			R-09	Kesalahan pada saat konfigurasi modem	Gangguan Jaringan	
5	Hardware	DVR1	R-10	Hilangnya pasokan daya atau listrik	Kerusakan Hardware	Proses yang bergantung dengan DVR menjadi terganggu
			R-11	Kesalahan dan kelalaian dalam melaksanakan prosedur kerja		
6	Hardware	Pendingin Ruangan (AC)	R-12	Proses perawatan aset tidak dilakukan dengan benar	Kerusakan Hardware	Temperatur ruangan terlalu tinggi dan dapat mengganggu kinerja server dan perangkat lain
			R-13	Pemantauan atau monitoring temperatur tidak dilakukan dengan maksimal	Human Error	
7	Hardware	Genset	R-14	Genset tidak berfungsi sebagaimana mestinya	Kegagalan Daya	Server down Jaringan internet tidak tersedia

ID	Kategori Aset	Nama Aset	Risk ID	Penyebab	Risiko	Dampak Langsung
				pada saat terjadi listrik padam		Proses bisnis terganggu
8	Hardware	UPS	R-15	Batrai UPS terbakar	Kebakaran	Kerusakan pada aset Kehilangan data Jaringan tidak tersedia
			R-16	Kesalahan konfigurasi sehingga UPS tidak berfungsi sebagaimana mestinya	Kegagalan Daya	Kerusakan pada aset Server down Proses yang bergantung dengan server terkait terganggu
9	Hardware	CCTV	R-17	Proses perawatan aset tidak dilakukan dengan benar	Kerusakan Hardware	Monitoring keamanan melalui cctv terganggu
10	Hardware	Panel Listrik	R-18	Hubungan arus pendek	Kebakaran	Kehilangan aset berupa hardware Kehilangan data Mengancam keselamatan SDM

ID	Kategori Aset	Nama Aset	Risk ID	Penyebab	Risiko	Dampak Langsung
			R-19	Gangguan pada panel listrik	Kegagalan Daya	Perangkat yang terhubung dengan panel listrik tersebut mati Layanan dari perangkat tertentu tidak tersedia
11	Network	Router	R-20	Kesalahan pada saat konfigurasi hardware	Gangguan Jaringan	Jaringan internet tidak tersedia
			R-21	Temperatur hardware terlalu tinggi (*overheat*)	Kerusakan Hardware	
12	Network	Telepon Kabel	R-22	Kesalahan dan kelalaian dalam melaksanakan prosedur kerja	Gangguan Jaringan	Jaringan telepon terganggu
13	Network	Kabel Fiber Optik	R-23	Penempatan kabel yang kurang baik	Kerusakan Hardware	Server down Proses yang berkaitan dengan server terganggu
			R-24	Perlindungan terhadap kabel yang kurang baik		
14	Network	PABX	R-25	Proses perawatan aset tidak dilakukan dengan benar	Gangguan Jaringan	Jaringan telepon terganggu

ID	Kategori Aset	Nama Aset	Risk ID	Penyebab	Risiko	Dampak Langsung
15	People	Staff	R-26	Kurangnya pengetahuan untuk prosedur penanganan gangguan pada server	Human Error	Down time server menjadi lama Proses yang berkaitan dengan server terkait terganggu
			R-27	Kesalahan prosedur kerja		
			R-28	Penyalahgunaan hak akses terhadap ruang server	Pencurian	Akses oleh pihak yang tidak berwenang Pencurian data Kehilangan data Kehilangan hardware Manipulasi data
			R-29	Meninggalkan ruangan dalam keadaan tidak terkunci		
			R-30	Pemberian hak akses yang tidak sesuai dengan prosedur kepada pihak tertentu	Pelanggaran Regulasi	

Dari hasil identifikasi risiko yang ditampilkan pada Tabel 5.6 diketahui bahwa terdapat beberapa risiko yang dapat dimasukkan ke dalam kategori yang sama yaitu :

1. Kerusakan Hardware
2. Gangguan Jaringan
3. Human Error
4. Kegagalan Daya
5. Kebakaran
6. Pencurian
7. Pelanggaran Regulasi

5.4.4 Penilaian Risiko

FMEA merupakan salah satu metode dalam melakukan penilaian terhadap risiko, metode ini menggunakan tiga aspek utama untuk menghasilkan sebuah nilai terhadap sebuah risiko. Ketiga aspek tersebut adalah tingkat keparahan (*severity*), frekuensi kejadian (*occurence*), dan juga keefektifan dari kontrol (*detection*) Dengan perhitungan nilai dari ketiga aspek ini maka akan menghasilkan sebuah *Risk Priority Number* (RPN) yang nantinya nilai RPN ini akan menunjukan sebuah risiko yang tergolong ke dalam kategori *Very High*, *High*, *Medium, Low*, dan juga *Very Low* seperti pada Tabel 2.3.

Proses penilaian risiko ini dilakukan bersama dengan Kepala Bagian TIK STIE Perbanas Surabaya, sehingga hasil penilaian yang diperoleh dapat dipercaya dan juga sesuai dengan penilaian dari pihak organisasi.

Tabel 5.7 Hasil Penilaian Risiko Menggunakan Metode FMEA

Kategori Aset	Nama Aset	Risk ID	Penyebab	Risiko	Occ	Dampak Langsung	Sev	Dampak Terhadap Bisnis	Det	Kontrol Terkini
Hardware	Server	R-01	Hilangnya pasokan daya atau listrik	Kerusakan Hardware	4	• Kerusakan pada asset • Server down • Kehilangan Data • Mengancam keselamatan	6	Proses bisnis yang bergantung dengan server terkait terganggu atau bahkan terhenti hingga server dapat pulih kembali	2	Penyediaan UPS dan Genset
		R-02	Temperatur ruangan terlalu tinggi (*Overheat*)		4		6		2	Pendingin Ruangan (AC) 2 buah
		R-03	Kesalahan konfigurasi dan perawatan hardware		3		7		3	Prosedur perawatan aset
		R-04	Bencana alam (petir, gempa bumi, angina kencang)		3		6		7	Pemasangan penagkal petir
Hardware	Monitor	R-05	Proses perawatan aset	Kerusakan Hardware	3	Kerusakan pada hardware	4	Kerugian finansial	3	Prosedur perawatan aset

Kategori Aset	Nama Aset	Risk ID	Penyebab	Risiko	Occ	Dampak Langsung	Sev	Dampak Terhadap Bisnis	Det	Kontrol Terkini
			tidak dilakukan dengan benar			Aktivitas yang bergantung dengan monitor terkait terganggu		untuk perbaikan atau pengadaan ulang		
		R-06	Kesalahan dan kelalaian dalam melaksanakan prosedur kerja		3		5		3	-
Hardware	Flash System Detector	R-07	Proses pearawatan aset tidak dilakukan dengan benar	Kerusakan Hardware	2	Hardware tidak dapat berfungsi	5	Proses bisnis terhenti jika terjadi kebakaran dan tidak bisa terdeteksi lebih dini	4	Prosedur perawatan aset
Hardware	Modem	R-08	Temperatur hardware terlalu tinggi (*overheat*)	Kerusakan Hardware	4	Jaringan internet terganggu	5	Proses bisis yang membutuhkan koneksi internet	3	Penyediaan pendingin ruangan (AC)
		R-09	Kesalahan pada saat konfigurasi modem	Gangguan Jaringan	3	Jaringan menjadi lemot	6		3	-

Kategori Aset	Nama Aset	Risk ID	Penyebab	Risiko	Occ	Dampak Langsung	Sev	Dampak Terhadap Bisnis	Det	Kontrol Terkini
						Jaringan tidak tersedia		(online) terganggu		
Hardware	DVR1	R-10	Hilangnya pasokan daya atau listrik	Kerusakan Hardware	3	Pemantauan keamanan terganggu	5	Proses bisnis yang bergantung dengan DVR menjadi terganggu	2	Penyediaan Genset dan UPS
		R-11	Kesalahan dan kelalaian dalam melaksanakan prosedur kerja		2		4		3	-
Hardware	Pendingin Ruangan (AC)	R-12	Proses perawatan aset tidak dilakukan dengan benar	Kerusakan Hardware	3	Temperatur ruangan menjadi naik atau tinggi dan dapat mengganggu kinerja server dan perangkat lain	5	Kerugian finansial untuk perbaikan atau pengadaan	3	Prosedur perawatan aset
		R-13	Pemantauan atau monitoring temperatur tidak dilakukan dengan maksimal	Human Error	4		6		3	

Kategori Aset	Nama Aset	Risk ID	Penyebab	Risiko	Occ	Dampak Langsung	Sev	Dampak Terhadap Bisnis	Det	Kontrol Terkini
Hardware	Genset	R-14	Genset tidak berfungsi sebagaimana mestinya pada saat listrik padam	Kegagalan Daya	4	Server down Jaringan internet tidak tersedia	7	Proses bisnis yang berhubungan langsung dengan server dan membutuhkan koneksi internet terganggu	5	Prosedur perawatan aset
Hardware	UPS	R-15	Batrai UPS terbakar	Kebakaran	2	Kerusakan pada aset Kehilangan data Jaringan tidak tersedia	9	Proses bisnis terhenti sampai batas waktu yang belum ditentukan	4	Pemasangan Flash System Detector
		R-16	Kesalahan konfigurasi sehingga UPS tidak berfungsi	Kegagalan Daya	3	Kerusakan pada aset Server down	6		5	-

Kategori Aset	Nama Aset	Risk ID	Penyebab	Risiko	Occ	Dampak Langsung	Sev	Dampak Terhadap Bisnis	Det	Kontrol Terkini
			sebagaimana mestinya			Proses yang bergantung dengan server terkait terganggu				
Hardware	CCTV	R-17	Proses perawatan aset tidak dilakukan dengan benar	Kerusakan Hardware	3	Monitoring keamanan melalui cctv terganggu	6	Keruggian finansial untuk perbaikan atau pengadaan	3	Prosedur perawatan aset
Hardware	Panel Listrik	R-18	Hubungan arus pendek	Kebakaran	2	Kehilangan aset berupa hardware Kehilangan data Mengancam keselamatan SDM	10	Proses bisnis terhenti sampai batas waktu yang belum ditentukan	3	Pemasangan smoke detectore

Kategori Aset	Nama Aset	Risk ID	Penyebab	Risiko	Occ	Dampak Langsung	Sev	Dampak Terhadap Bisnis	Det	Kontrol Terkini
		R-19	Gangguan pada panel listrik	Kegagalan Daya	3	Perangkat yang terhubung dengan panel listrik tersebut mati Layanan dari perangkat tertentu tidak tersedia	7		4	Penyediaan Genset
Network	Router	R-20	Kesalahan pada saat konfigurasi hardware	Gangguan Jaringan	3	Jaringan internet tidak tersedia	5	Proses bisnis yang membutuhkan koneksi internet terganggu	3	-
		R-21	Temperatur hardware terlalu tinggi (*overheat*)	Kerusakan Hardware	3		5		3	Penyediaan pendingin ruangan (AC)
Network	Telepon Kabel	R-22	Kesalahan dan kelalaian dalam	Gangguan Jaringan	3	Jaringan telepon terganggu	6	Layanan melalui	3	-

Kategori Aset	Nama Aset	Risk ID	Penyebab	Risiko	Occ	Dampak Langsung	Sev	Dampak Terhadap Bisnis	Det	Kontrol Terkini
			melaksanakan prosedur kerja					telepon terganggu		
Network	Kabel Fiber Optik	R-23	Penempatan kabel yang kurang baik	Kerusakan Hardware	3	Server down	6	Proses yang berkaitan dengan server terganggu	3	Ditempatkan di bawah lantai
		R-24	Perlindungan terhadap kabel yang kurang baik		3		6		4	Kabel dilapisi dengan pipa
Network	PABX	R-25	Proses perawatan aset tidak dilakukan dengan benar	Gangguan Jaringan	2	Jaringan telepon terganggu	5	Layanan melalui telepon terganggu	3	Prosedur perawatan aset
People	Staff	R-26	Kurangnya pengetahuan untuk prosedur penanganan gangguan pada server	Human Error	3	Down time server menjadi lama Proses yang berkaitan dengan server	6	Reputasi yang kurang baik dari *client.*	3	-

Kategori Aset	Nama Aset	Risk ID	Penyebab	Risiko	Occ	Dampak Langsung	Sev	Dampak Terhadap Bisnis	Det	Kontrol Terkini
		R-27	Kesalahan prosedur kerja		3	terkait terganggu	7		3	-
		R-28	Penyalahgunaan hak akses terhadap ruang server	Pencurian	5	Akses oleh pihak yang tidak berwenang Kehilangan data Kehilangan hardware Manipulasi data	6		4	Pemasangan kamera pengawas Kunci ruangan
		R-29	Meninggalkan ruangan dalam keadaan tidak terkunci		4		6		3	Pemasangan kamera pengawas
		R-30	Pemberian hak akses yang tidak sesuai dengan prosedur kepada pihak tertentu	Pelanggaran Regulasi	3		5		4	Pemasangan kamera pengawas Kunci ruangan

Tabel 5.8 Nilai RPN dan Level Risiko

Kategori Aset	Nama Aset	Risk ID	Penyebab	Risiko	Occ	Sev	Det	RPN	Level RPN
Hardware	Server	R-01	Hilangnya pasokan daya atau listrik	Kerusakan Hardware	4	6	2	48	Low
		R-02	Temperatur ruangan terlalu tinggi (*Overheat*)		4	6	2	48	Low
		R-03	Kesalahan konfigurasi dan perawatan hardware		3	7	3	63	Low
		R-04	Bencana alam (petir, gempa bumi, angina kencang)		3	6	7	126	High
Hardware	Monitor	R-05	Proses perawatan aset tidak dilakukan dengan benar	Kerusakan Hardware	3	4	3	36	Low
		R-06	Kesalahan dan kelalaian dalam melaksanakan prosedur kerja		3	5	3	45	Low
Hardware	Flash System Detector	R-07	Proses pearawatan aset tidak dilakukan dengan benar	Kerusakan Hardware	2	5	4	40	Low

Kategori Aset	Nama Aset	Risk ID	Penyebab	Risiko	Occ	Sev	Det	RPN	Level RPN
Hardware	Modem	R-08	Temperatur hardware terlalu tinggi (*overheat*)	Kerusakan Hardware	4	5	3	60	Low
		R-09	Kesalahan pada saat konfigurasi modem	Gangguan Jaringan	3	6	3	54	Low
Hardware	DVR1	R-10	Hilangnya pasokan daya atau listrik	Kerusakan Hardware	3	5	2	30	Low
		R-11	Kesalahan dan kelalaian dalam melaksanakan prosedur kerja		2	4	3	24	Low
Hardware	Pendingin Ruangan (AC)	R-12	Proses perawatan aset tidak dilakukan dengan benar	Kerusakan Hardware	3	5	3	45	Low
		R-13	Pemantauan atau monitoring temperatur tidak dilakukan dengan maksimal	Human Error	4	6	3	72	Low
Hardware	Genset	R-14	Genset tidak berfungsi sebagaimana mestinya	Kegagalan Daya	4	7	5	140	High

Kategori Aset	Nama Aset	Risk ID	Penyebab	Risiko	Occ	Sev	Det	RPN	Level RPN
			pada saat terjadi listrik padam						
Hardware	UPS	R-15	Batrai UPS terbakar	Kebakaran	2	9	4	72	Low
		R-16	Kesalahan konfigurasi sehingga UPS tidak berfungsi sebagaimana mestinya	Kegagalan Daya	3	6	5	90	Medium
Hardware	CCTV	R-17	Proses perawatan aset tidak dilakukan dengan benar	Kerusakan Hardware	3	6	3	54	Low
Hardware	Panel Listrik	R-18	Hubungan arus pendek	Kebakaran	2	10	3	60	Low
		R-19	Gangguan pada panel listrik	Kegagalan Daya	3	7	4	84	Medium
Network	Router	R-20	Kesalahan pada saat konfigurasi hardware	Gangguan Jaringan	3	5	3	45	Low
		R-21	Temperatur hardware terlalu tinggi (*overheat*)	Kerusakan Hardware	3	5	3	45	Low

Kategori Aset	Nama Aset	Risk ID	Penyebab	Risiko	Occ	Sev	Det	RPN	Level RPN
Network	Telepon Kabel	R-22	Kesalahan dan kelalaian dalam melaksanakan prosedur kerja	Gangguan Jaringan	3	6	3	54	Low
Network	Kabel Fiber Optik	R-23	Penempatan kabel yang kurang baik	Kerusakan Hardware	3	6	3	54	Low
		R-24	Perlindungan terhadap kabel yang kurang baik		3	6	4	72	Low
Network	PABX	R-25	Proses perawatan aset tidak dilakukan dengan benar	Gangguan Jaringan	2	5	3	30	Low
People	Staff	R-26	Kurangnya pengetahuan untuk prosedur penanganan gangguan pada server	Human Error	3	6	3	54	Low
		R-27	Kesalahan prosedur kerja		3	7	3	63	Low
		R-28	Penyalahgunaan hak akses terhadap ruang server	Pencurian	5	6	4	120	High

Kategori Aset	Nama Aset	Risk ID	Penyebab	Risiko	Occ	Sev	Det	RPN	Level RPN
		R-29	Meninggalkan ruangan dalam keadaan tidak terkunci		4	6	3	72	Low
		R-30	Pemberian hak akses yang tidak sesuai dengan prosedur kepada pihak tertentu	Pelanggaran Regulasi	3	5	4	60	Low

Secara garis besar, hasil penialian risiko dengan menggunakan metode FMEA yang dilakukan bersama dengan Kepala Bagian TIK STIE Perbanas Surabaya menunjukan kebanyakan risiko berada pada level *Low* dimana risiko yang berada pada level *Low* berjumlah 25, level *Medium* sejumlah 2 risiko, dan level *High* sejumlah 3 risiko.

Hal ini menunjukan beberapa risiko sudah memiliki kontrol yang cukup tepat untuk mengantisipasi maupun menangani risiko tersebut. Untuk memastikan risiko yang berhasil diidentifikasi telah dalam penangan yang sesuai perlu dilakukan pemeriksaan terhadap kontrol yang sudah ada untuk setiap risikonya.

5.5 Pemetaan Risiko dengan Kontrol ISO/IEC 27002:2013 Klausul Keamanan Fisik dan Lingkungan

Hasil dari penilaian risiko menggunakan metode FMEA selanjutnya dipetakan ke dalam control ISO/IEC 27002:2013 klausul keamanan fisik dan lingkungan dengan menghubungkan antara risiko, penyebab dari risiko terhadap *implementation guidence* untuk kontrol yang ada pada klausul 11 (klausul keamanan fisik dan lingkungan). Hasil pemetaan ini akan menunjukan apakah organisasi sudah mengimplementasikan kontrol yang tepat dan sesuai untuk menangani atau menanggulangi risiko terkait. Hasil dari pemetaan risiko dengan kontrol yang ada dapat di lihat pada Tabel 5.9 berikut ini.

Tabel 5.9 Pemetaan Risiko dengan Kontrol ISO/IEC 27002:2013 Klausul Keamanan Fisik dan Lingkungan

Kategori Aset	Nama Aset	Risk ID	Penyebab	Risiko	Kontrol ISO/IEC 27002:2013
Hardware	Server	R-01	Hilangnya pasokan daya atau listrik	Kerusakan Hardware	*11.2.2 Supporting Utilities*
		R-02	Temperatur ruangan terlalu tinggi (*Overheat*)		*11.2.2 Supporting Utilities* *11.2.1 Equipment siting and protection*
		R-03	Kesalahan konfigurasi dan perawatan hardware		*11.2.4 Equipment maintenance*
		R-04	Bencana alam (petir, gempa bumi, angina kencang)		*11.1.4 Protecting against external and environmental threats*
Hardware	Monitor	R-05	Proses perawatan aset tidak dilakukan dengan benar	Kerusakan Hardware	*11.2.4 Equipment maintenance*

Kategori Aset	Nama Aset	Risk ID	Penyebab	Risiko	Kontrol ISO/IEC 27002:2013
		R-06	Kesalahan dan kelalaian dalam melaksanakan prosedur kerja		*11.2.4 Equipment maintenance*
Hardware	Flash System Detector	R-07	Proses pearawatan aset tidak dilakukan dengan benar	Kerusakan Hardware	*11.2.4 Equipment maintenance*
Hardware	Modem	R-08	Temperatur hardware terlalu tinggi (*overheat*)	Kerusakan Hardware	*11.2.1 Equipment siting and protection*
		R-09	Kesalahan pada saat konfigurasi modem	Gangguan Jaringan	*11.2.1 Equipment siting and protection*
Hardware	DVR1	R-10	Hilangnya pasokan daya atau listrik	Kerusakan Hardware	*11.2.2 Supporting Utilities*
		R-11	Kesalahan dan kelalaian dalam		*11.2.4 Equipment maintenance*

Kategori Aset	Nama Aset	Risk ID	Penyebab	Risiko	Kontrol ISO/IEC 27002:2013
			melaksanakan prosedur kerja		
Hardware	Pendingin Ruangan (AC)	R-12	Proses perawatan aset tidak dilakukan dengan benar	Kerusakan Hardware	*11.2.4 Equipment maintenance*
		R-13	Pemantauan atau monitoring temperatur tidak dilakukan dengan maksimal	Human Error	*11.2.1 Equipment siting and protection*
Hardware	Genset	R-14	Genset tidak berfungsi sebagaimana mestinya pada saat terjadi listrik padam	Kegagalan Daya	*11.2.2 Supporting Utilities*
Hardware	UPS	R-15	Batrai UPS terbakar	Kebakaran	*11.1.4 Protecting against external and environmental threats*

Kategori Aset	Nama Aset	Risk ID	Penyebab	Risiko	Kontrol ISO/IEC 27002:2013
					11.2.2 Supporting Utilities
		R-16	Kesalahan konfigurasi sehingga UPS tidak berfungsi sebagaimana mestinya	Kegagalan Daya	*11.2.1 Equipment siting and protection*
Hardware	CCTV	R-17	Proses perawatan aset tidak dilakukan dengan benar	Kerusakan Hardware	*11.2.4 Equipment maintenance*
Hardware	Panel Listrik	R-18	Hubungan arus pendek	Kebakaran	*11.2.3 Cabling security*
		R-19	Gangguan pada panel listrik	Kegagalan Daya	*11.2.2 Supporting Utilities*
Network	Router	R-20	Kesalahan pada saat konfigurasi hardware	Gangguan Jaringan	*11.2.1 Equipment siting and protection*

Kategori Aset	Nama Aset	Risk ID	Penyebab	Risiko	Kontrol ISO/IEC 27002:2013
		R-21	Temperatur hardware terlalu tinggi (*overheat*)	Kerusakan Hardware	*11.2.1 Equipment siting and protection*
Network	Telepon Kabel	R-22	Kesalahan dan kelalaian dalam melaksanakan prosedur kerja	Gangguan Jaringan	*11.2.4 Equipment maintenance*
Network	Kabel Fiber Optik	R-23	Penempatan kabel yang kurang baik	Kerusakan Hardware	*11.2.3 Cabling security*
		R-24	Perlindungan terhadap kabel yang kurang baik		*11.2.3 Cabling security* *11.2.1 Equipment siting and protection*
Network	PABX	R-25	Proses perawatan aset tidak dilakukan dengan benar	Gangguan Jaringan	*11.2.4 Equipment maintenance*
People	Staff	R-26	Kurangnya pengetahuan untuk prosedur	Human Error	*11.2.4 Equipment maintenance*

Kategori Aset	Nama Aset	Risk ID	Penyebab	Risiko	Kontrol ISO/IEC 27002:2013
			penanganan gangguan pada server		
		R-27	Kesalahan prosedur kerja		*11.1.5 Working in secure areas*
		R-28	Penyalahgunaan hak akses terhadap ruang server	Pencurian	*11.1.2 Physical entry controls*
		R-29	Meninggalkan ruangan dalam keadaan tidak terkunci		*11.1.2 Physical entry controls*
		R-30	Pemberian hak akses yang tidak sesuai dengan prosedur kepada pihak tertentu	Pelanggaran Regulasi	*11.1.2 Physical entry controls*

Dari proses pemetaan yang dilakukan, didapatkan 7 kontrol untuk keamanan fisik dan lingkungan sesuai dengan *Control Objective* ISO/IEC 27002:2013. Tujuh kontrol iniliah yang nantinya digunakan sebagai acuan dalam pembuatan dokumen *audit program* yakni pada pembuatan perangkat audit.

5.6 Penyusunan Dokumen *Audit Program*

Dalam penyusunan dokumen audit program untuk Bagian TIK STIE Perbanas Surabaya berdasarkan ISO/IEC 27002:2013 klausul keamanan fisik dan lingkungan, penulis menggunakan dokumen dari penelitian yang dilakukan oleh Stephen [4] sebagai acuan dalam membuat perangkat audit.

5.6.1 Kerangka Dokumen

Struktur dan isi dari dokumen *audit program* yang dibuat penulis kali ini adalah sebagai berikut.

1. **Informasi Umum**
   Informasi umum pada audit program ini berisikan informasi atau pengetahuan umum terkait dengan audit yang akan dilakukan. Adapun isi dari informasi umum secara lebih detail adalah sebagai berikut :
   a. Tujuan
      Berisikan tujuan dari pembuatan dokumen *audit program* yang diperoleh dari hasil studi literatur menggunakan hasil penelitian yang menghasilkan dokumen serupa..
   b. Analisis Risiko
      Berisikan hasil analisis risiko yang sudah dilakukan oleh penulis sebelumnya dengan ruang lingkup yang sudah ditentukan yakni risiko terkait keamanan fisik dan lingkungan teknologi informasi terhadap aset yang ada di ruang server.
   c. Control Objective

Daftar dari *control objective* ISO 27002:2013 klausul 11 yaitu Kemanan Fisik dan Lingkungan yang sudah disesuaikan dengan hasil analisis risiko sehingga didapatkan 7 kontrol.

d. Dokumen Acuan Kerja
   Berisikan daftar dokumen yang sekiranya dibutuhkan serta dapat membantu dan memudahkan Auditor dalam melaksanakan pemeriksaan.
e. Proses Audit
   Berisikan garis besar mengenai proses audit yang seharusnya dilewati oleh auditor ketika melakukan pemeriksaan.

2. Penilaian Risiko
Pada bagian ini berisikan hasil penilaian risiko yang sudah dilakukan oleh penulis. Bagian ini bertujuan untuk membantu auditor dalam memberikan prioritas pada kontrol mana saja yang harus lebih diperhatikan berdasarkan atas nilai RPN untuk setiap risikonya.

3. Perangkat Audit
Perangkat audit merupakan bagian dari dokumen *audit program* yang berisikan daftar kontrol yang harus diperiksa oleh auditor.

Untuk isi yang lebih lengkap dari dokumen ini dapat dilihat pada buku produk dokumen *Audit Program*.

5.6.2 Pembuatan Perangkat Audit

Dalam pembuatan perangkat audit, terdapat aturan dalam penamaan dokumen serta penamaan komponen yang ada di dalamnya.

1. Aturan Penamaan Dokumen
Dengan adanya penamaan dokumen prosedur audit akan mempermudah dalam penggunaan dokumen nantinya.

Komposisi dalam penamaan dokumen prosedur audit adalah seperti berikut ini.

a. Nama Dokumen
- P = Prosedur Audit
- PTL = Pelaksanaan Tindak Lanjut Temuan

b. Nomor Sub Klausul Kontrol terkait
c. Nomor *Control Objective* dari sub klausul

Contoh penamaan dokumen :
Dokumen yang akan dibuat adalah Prosedur Audit terkait kontrol 11.2.2 *Supporting Utilities.*

Untuk dokumen prosedur audit memiliki kode **P**, dan kontrol tersebut berasal dari sub klausul **2** serta merupakan kontrol objektif yang kedua (**2**). Sehingga, penamaannya akan menjadi **P.2.2**.

2. Komponen Dokumen *Perangkat Audit*

a. *Daftar Perangkat Audit*

Pada perangkat audit terdapat 7 dokumen yang sudah disusun berdasarkan kontrol objektif pada standar ISO/IEC 27002:2013 untuk klausul Keamanan Fisik dan Lingkungan. Daftar dokumen perangkat audit yang ada dapat dilihat pada Tabel 5.9 berikut ini.

Tabel 5.9 Daftar Perangkat Audit

No.	ID Dokumen	Nama Dokumen
1.	P.1.2	*11.1.2 Physical entry controls*
2.	P.1.4	*11.1.4 Protecting against external and environmental threats*
3.	P.1.5	*11.1.5 Working in secure areas*
4.	P.2.1	*11.2.1 Equipment sitting and protection*

No.	ID Dokumen	Nama Dokumen
5.	P.2.2	*11.2.2 Supporting Utilities*
6.	P.2.3	*11.2.3 Cabling security*
7.	P.2.4	*11.2.4 Equipment maintenance*

Prosedur audit dibuat berdasarkan *implementation guidance* yang ada pada setiap *control objective* ISO/IEC 27002:2013 untuk klausul keamanan fisik dan lingkungan yang sudah ditentukan seperti pada Tabel 5.9.

Dari 7 kontrol di ISO/IEC 27002:2013 pada klausul keamanan fisik dan lingkungan yang digunakan untuk menyusun perangkat audit, dihasilkan prosedur dan daftar cek audit dengan detail sebagai berikut :

11.1.2 *Physycal Entry Control*

Pada kontrol ini terdapat 4 poin prosedur audit dengan 13 *Checklist* sebagai berikut :

- Prosedur 1
  Prosedur ini memiliki 4 *checklist* dengan nomor a, b, c, dan d.
- Prosedur 2
  Prosedur ini memiliki 2 *checklist* dengan nomor a dan b.
- Prosedur 3
  Prosedur ini memiliki 4 checklist dengan nomor a, b, c, dan d.
- Prosedur 4
  Prosedur ini memiliki 3 checklist dengan nomor a, b, dan c.

11.1.4 *Protecting Against External and Environmental Threats*

Pada kontrol ini terdapat 3 poin prosedur audit dengan 9 *checklist* sebagai berikut :

- Prosedur 1
  Prosedur ini memiliki 3 *checklist* dengan nomor a, b, dan c.
- Prosedur 2
  Prosedur ini memiliki 2 *checklist* dengan nomor a dan b.
- Prosedur 3
  Prosedur ini memiliki 4 *checklist* dengan nomor a, b, c dan d.

11.1.5 *Working in Secure Areas*

Pada kontrol ini terdapat 4 poin prosedur audit dengan 10 *checklist* sebagai berikut :

- Prosedur 1
  Prosedur ini memiliki 3 *checklist* dengan nomor a, b, dan c.
- Prosedur 2
  Prosedur ini memiliki 2 *checklist* dengan nomor a dan b.
- Prosedur 3
  Prosedur ini memiliki 3 *checklist* dengan nomor a, b dan c.
- Prosedur 4
  Prosedur ini memiliki 2 *checklist* dengan nomor a dan b.

11.2.1 *Equipment Sitting and Protection*

Pada kontrol ini terdapat 4 poin prosedur audit dengan 14 *checklist* sebagai berikut :

- Prosedur 1
  Prosedur ini memiliki 4 *checklist* dengan nomor a, b, c, dan d.
- Prosedur 2

Prosedur ini memiliki 4 *checklist* dengan nomor a, b, c dan d.

- Prosedur 3
  Prosedur ini memiliki 4 *checklist* dengan nomor a, b, c dan d.
- Prosedur 4
  Prosedur ini memiliki 2 *checklist* dengan nomor a dan b.

11.2.2 *Supporting Utilities*

Pada kontrol ini terdapat 5 poin prosedur audit dengan 15 *checklist* sebagai berikut :

- Prosedur 1
  Prosedur ini memiliki 5 *checklist* dengan nomor a, b, c, d dan e.
- Prosedur 2
  Prosedur ini memiliki 2 *checklist* dengan nomor a dan b.
- Prosedur 3
  Prosedur ini memiliki 4 *checklist* dengan nomor a, b, c, dan d.
- Prosedur 4
  Prosedur ini memiliki 2 *checklist* dengan nomor a dan b.
- Prosedur 5
  Prosedur ini memiliki 2 *checklist* dengan nomor a dan b.

11.2.3 *Cabling Security*

Pada kontrol ini terdapat 2 poin prosedur audit dengan 5 *checklist* sebagai berikut :

- Prosedur 1
  Prosedur ini memiliki 2 *checklist* dengan nomor a dan b
- Prosedur 2

Prosedur ini memiliki 3 *checklist* dengan nomor a, b, dan c.

11.2.4 *Equipment Maintenance*

Pada kontrol ini terdapat 6 poin prosedur audit dengan 15 *checklist* sebagai berikut :

- Prosedur 1
  Prosedur ini memiliki 2 *checklist* dengan nomor a dan b.
- Prosedur 2
  Prosedur ini memiliki 2 *checklist* dengan nomor a dan b.
- Prosedur 3
  Prosedur ini memiliki 3 *checklist* dengan nomor a, b, dan c.
- Prosedur 4
  Prosedur ini memiliki 2 *checklist* dengan nomor a dan b.
- Prosedur 5
  Prosedur ini memiliki 2 *checklist* dengan nomor a dan b.
- Prosedur 6
  Prosedur ini memiliki 1 *checklist* dengan nomor a.

b. *Audit Checklist*

Untuk setiap *prosedur audit* yang ada akan dijabarkan lagi ke dalam beberapa langkah – langkah pemeriksaan yang tersusun di dalam *audit checklist. Audit checklist* berisikan daftar pertanyaan yang dibagi menjadi 2 yaitu pertanyaan *compliance* dan *substantive*. Pertanyaan *compliance* berisikan pertanyaan tentang ketersediaan akan sesuatu baik itu berupa dokumen, barang, informasi dan lainnya, sedangkan jenis *substantive* menanyakan kesesuaian akan suatu hal yang dapat berupa peraturan, kebijakan, ataupun prosedur yang ada.

Pada *audit checklist* juga berisikan sebuah kolom "Evidence" yang akan diisi oleh auditor dengan bukti – bukti baik berupa dokumen, foto, atau bentuk lain yang didapatkan oleh auditor terkait dengan pertanyaan pada kolom *audit checklist.*

Salah satu contoh prosedur audit untuk *Control Objective* 11.2.2 *Supporting Utilities* dapat dilhat pada Gambar 5.1 berikut ini.

STIE Perbanas www.perbanas.ac.id	PROSEDUR AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI RUANG SERVER STIE PERBANAS SURABAYA		
	11.2.2 Supporting Utillities	P.2.2	
	Peralatan harus dilindungi dari gangguan listrik dan gangguan lain yang disebabkan oleh kegagalan dari sarana pendukung.	AUDITOR *ttd* (Nama Auditor)	AUDITEE *ttd* (Nama Auditee)
TANGGAL & WAKTU :			

Audit Procedure	Testing	Audit Checklist	Yes	No	Partial	Evidence
Auditor melakukan pengecekan terhadap sarana pendukung yang digunakan untuk menunjang aset yang ada di ruang server. 1. Auditor mencari dan mengumpulkan informasi serta melakukan observasi mengenai peralatan berupa sarana pendukung yang menunjang aset di raung server	**Compliance**	a. Apakah perusahaan/organisasi sudah memiliki generator pembangkit tenaga listrik yang dapat menyediakan daya listrik ketika terjadi pemadaman?				Dokumen daftar aset Foto genset
	Compliance	b. Jika ada, apakah terdapat dokumen untuk spesifikasi generator pembangkit tenaga listrik yang dimaksud?				Dokumen spesifikasi alat
	Compliance	c. Apakah perusahaan/organisasi sudah memiliki UPS (*Uninterruptible Power Supply*) untuk menjaga peralihan daya listrik ke generator ketika terjadi pemadaman?				Dokumen daftar aset Foto UPS
	Compliance	d. Jika ada, apakah terdapat dokumen untuk spesifikasi dari UPS tersebut?				Dokumen spesifikasi alat

Gambar 5.1 Contoh *Prosedur Audit*

c. Formulir Laporan Pemeriksaan

Untuk memudahkan auditor dalam merangkum dan menjelaskan temuan selama pemeriksaan untuk sebuah kontrol yang telah dilakukan, maka dibuatkanlah sebuah formulir laporan pemeriksaan. Dalam pembuataannya, formulir laporan pemeriksaan ini mengacu pada standar ISO 19011 [13], dimana pada standar ini menjelaskan bahwa dalam melakukan audit, waktu, objek pelaksanaan,

dan juga tim pemeriksa atau auditor harus didefinisikan dengan jelas. Berdasarkan atas informasi tersebut, maka dalam pembuatan formulir laporan pemeriksaan akan berisikan kolom untuk "Tanggal Pemeriksaan" yang harus diisikan oleh auditor dengan informasi mengenai waktu pelaksanaan pemeriksaan terkait, kolom "Auditor" yang harus diisi dengan informasi nama dari pelaksana audit, serta kolom "Auditee" yang harus diisikan dengan informasi mengenai nama unit atau orang yang sedang diperiksa atau diaudit. Selain hal tersebut, standar ISO 19011 juga membahas mengenai proses menghasilkan temuan audit. Temuan audit merupakan salah satu hal yang sangat penting dalam proses audit sehingga pada formulir laporan pemeriksaan akan terdapat kolom "Kesimpulan" yang harus diisikan dengan temuan ketidaksesuaian terhadap suatu kontrol yang diperiksa oleh auditor.

Pada ISO 19011 terkait dengan proses audit yang keenam yaitu *audit follow-up* membahas mengenai tindak lanjut terhadap hasil temuan selama porses audit berlangsung. Tindak lanjut ditentukan ketika proses pemeriksaan telah selesai dilakukan, sehingga pada formulir laporan pemeriksaan juga berisikan kolom "Usulan Tindak Lanjut" yang harus diisi oleh auditor dengan saran perbaikan untuk agar temuan yang ada dapat diatasi. Untuk memastikan agar saran perbaikan lebih diperhatikan dan dilaksanakan maka dibuatkan kolom "Batas Penyelesaian Perbaikan" serta "Penanggung Jawab". Kolom "Batas Penyelesaian Perbaiakan" diisi dengan informasi mengenai batas waktu (*deadline*) dalam penyelesaian saran perbaikan yang diberikan, dan kolom "Penanggung Jawab" diisi dengan nama orang yang

bertanggung jawab untuk pelaksanaan perbaikan terkait.

Pada formulir laporan pemeriksaan juga berisikan sebuah kolom “Pengesahan”. Hal ini menagcu dari ISO 19011 pada bagian *planning* [13], yang menyatakan sebuah temuan yang diperoleh pada setiap kontrol haruslah disetujui oleh kedua belah pihak, yaitu pihak *auditor* dan *auditee.* Sehingga pada kolom “Pengesahan” akan diisi dengan nama serta tanda tangan dari *auditor* dan *auditee*. Ketika proses pengesahan ini telah dilakukan, maka pihak organisasi akan menerima apa saja yang telah dituliskan oleh auditor, dan akan melaksanakan proses perbaikan dengan batas waktu yang juga sudah ditentukan.

Di lain sisi, audit berbasis risiko bertujuan untuk memastikan bahwa risiko telah dikelola dalam batasan risiko yang sudah ditetapkan oleh pihak manajemen pada tingkatan koorporasi [21], sehingga perlu adanya penilaian terhadap kontrol yang telah diterapkan organisasi terhadap suatu risiko. Dari hal ini, dibuatkanlah kolom “Risiko Terkait” yang berisi “Risiko”, “Detect”, “RPN” dan “Level”. Untuk “Risiko” diisi dengan ID dari risiko berdasarkan tabel *Risk Register,* “Detect” diisi dengan nilai *detection* pada tabel hasil penilaian risiko, “RPN” diisi dengan nilai RPN, serta “Level” diisi dengan level risiko terkait berdasarkan FMEA.

Pada Gambar 5.2 berikut merupakan contoh dari sebuah formulir laporan pemeriksaan untuk *Control Obejctive* 11.2.2 *Supporting Utilities* yang terdapat pada dokumen audit program.

LAPORAN PEMERIKSAAN No Temuan : TP.1.2					
Tanggal Pemeriksaan : (dd/mm/yyyy)	**Auditor :** (Tuliskan nama Auditor pemeriksa control ini)			**Auditee :** (Tuliskan nama Auditee)	
Klausul : ***11.1.2 Physical entry control***				**Risiko Terkait :**	
Kesimpulan : (Tuliskan kesimpulan temuan auditor terhadap aktivitas yang diaudit di perusahaan/organisasi yang juga mengacu pada hirarki prosedur audit)				**Risiko**	**Detect**
Usulan Tindak Lanjut : (Tuliskan usulan tindak lanjut dari auditor terkait dengan temuan)				**Batas Penyelesaian Perbaikan :** (Tuliskan batas waktu untuk menyelesaikan tindak lanjut)	
				Penanggung Jawab : (Tuliskan penanggung jawab terhadap tindakan perbaikan ini)	

Gambar 5.2 Contoh Formulir Laporan Pemeriksaan

5.6.3 Pembuatan Formulir Pelaksanaan Tindak Lanjut

Tahapan selanjutnya dalam pembauatan audit program adalah membuat form pelaksanaan tindak lanjut. Secara umum form pelaksanaan tindak lanjut adalah sebuah formulir yang berisikan informasi mengenai tindak lanjut yang dilakukan oleh pihak organisasi terkait dengan temuan selama proses audit berlangsung. Formulir pelaksanaan tindak lanjut ini harus diisikan oleh pihak organisasi.

Pada formulir pelaksanaan tindak lanjut akan berisikan kolom "Tanggal Audit" yang diisikan dengan informasi mengenai waktu pelaksanaan audit terhadap kontrol terkait yang ada pada kolom "Nama Kontrol" dilaksanakan. Terdapat juga kolom "Pelaksana" yang diisi dengan nama unit atau orang yang melaksanakan perbaikan tersebut, dimana hal ini akan dicocokkan dengan Formulir Laporan Pemeriksaan untuk memastikan kesesuaiannya. Selain itu, pada formulir pelaksanaan tindak lanjut juga berisikan kolom lainnya yaitu kolom "Pelaksanaan Tindak Lanjut", "Tanggal Penyelesaian", dan "Pengesahan". Kolom "Pelaksanaan Tindak Lanjut" diiskan dengan tindakan yang telah dilakukan oleh pihak organisasi terhadap temuan pada kontrol tertentu, sehingga dapat diketahui oleh pihak *auditor*. Untuk kolom "Tanggal Penyelesaian" diisikan dengan informasi mengenai waktu dari

tindak lanjut yang telah dilakukan, apakah sudah sesuai dengan *deadline* yang ditetapkan auditor sebelumnya. Kolom "Pengesahan" disertakan sebagai verifikasi antara pihak pelaksana, auditor, dan juga direktur yang menyatakan bahwa perbaikan telah dilaksanakan.

Gambar 5.3 berikut ini menunjukan sebuah formulir pelaksanaan tindak lanjut.

FORMULIR AUDIT FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI RUANG SERVER STIE PERBANAS SURABAYA	STIE Perbanas www.perbanas.ac.id
Pelaksanaan Tindak Lanjut Internal No. Program :	
Tanggal Audit : [DD-MM-YYYY]	**Nama Kontrol** : [isikan sesuai dengan nama kontrol]
Pelaksana : [isikan nama pelaksana]	
Pelaksanaan : [isikan program yang telah dilakukan oleh organisasi]	
Tanggal Penyelesaian : [DD-MM-YYYY]	
Pengesahan Pelaksana : Auditor : Kepala Bagian TIK : (.....) (.....) (.....)	

Gambar 5.3 Formulir Pelaksanaan Tindak Lanjut

5.6.4 Pembuatan Panduan Penggunaan Perangkat Audit

Pada tahapan ini akan dibuat dokumen panduan penggunaan untuk dokumen audit program yang sudah ada khususnya untuk bagian perangkat audit. Adapun isi dari dokumen penduan penggunaan ini adalah sebagai berikut :

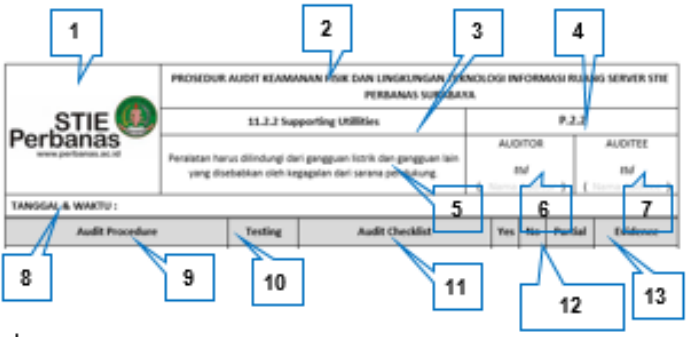
1. **Pendahuluan**
   Bagian ini berisikan latar belakang pembuatan dokumen panduan penggunaan audit program serta daftar dari perangat audit yang telah dibuat.
2. **Panduan Umum**
   Pada bagian ini dijelaskan mengenai petunjuk – petunjuk umum dalam penggunaan dokumen audit program. Petunjuk yang dimaksud adalah tat acara pengisian maupun penggunaan dari seluruh dokumen audit program. Panduan umum ini terdiri dari :
   a. Petunjuk Pengisian Perangkat Audit
   b. Petunjuk Pengisian Laporan Pemeriksaan
   c. Petunjuk Pengisian Tindak Lanjut Temuan Audit.
3. **Panduan Khusus**
   Bagian ini berisikan informasi mengenai panduan penggunaan yang bersifat khusus yang menjelaskan dokumen apa saja yang akan dibutuhkan oleh pihak auditor pada saat melaksanakan pemeriksaan.
4. **Pengecualian**
   Bagian pengecualian menjelaskan mengenai pengecualian untuk penggunaan dokumen ini. Dokumen panduan ini dibuat berdasarkan dokumen audit program yang telah dibuat oleh penulis sebelumnya.

Gambar 5.4 berikut ini merupakan contoh dari isi dokumen panduan penggunaan audit program.

4.2 Panduan Umum

4.2.1 Petunjuk Penggunaan Prosedur Audit

Sebelum dapat memahami tata cara dan urutan untuk pengisian prosedur audit akan lebih baik jika mengerti bagian – bagian prosedur dari audit yang tersedia, terutama bagian header. Berikut ini merupakan bagian header dari prosedur audit.



Berikut ini adalah penjelasan untuk setiap penomeran pada header yang ada pada gambar di atas.

No.	Definisi
1	Logo dari STIE Perbanas Surabaya
2	Header yang berisikan penjelasan dokumen prosedur audit keamanan fisik dan lingkungan teknologi informasi
3	Nama bagian dokumen dimana setiap dokumen akan memiliki nama yang berbeda sesuai dengan ketentuan yang telah diberikan
4	Nomor dokumen audit checklist, dimana pemberian nomor ini mengikuti pemberian nomor dari control objective dokumen terkait.
	P : Prosedur Audit
	2 : Control Objective 2
5	Penjelasan dari control yang dikelola oleh Control Objective pada dokumen tersebut.
6	Identitas dan tanda tangan Lead Auditor yang bertugas pada saat pemeriksaan.
7	Identitas dan tanda tangan ama Auditee yang berlan dengan control pada saat dilakukan proses audit.
8	Tanggal dan waktu berlangsungnya pemeriksaan terhadap kontrol.
9	Berisikan tata urutan prosedur untuk setiap langkah dalam memastikan audit dari setiap Control Objective.
10	Jenis testing yang akan dilakukan untuk setiap instruksinya. Terdapat 2 jenis testing yang akan digunakan yaitu Substantive dan Compliance.

Gambar 5.4 Contoh Isi Panduan Penggunaan Audit Program

5.7 Verfikasi Dokumen *Audit Program*

Verifikasi audit program yang dimaksudkan di sini adalah proses verifikasi terhadap perangkat audit yang berisikan prosedur dan *checklist* audit dengan cara melakukan *traceback* ke kontrol pada standar ISO/IEC 27002:2013 untuk klausul keamanan fisik dan lingkungan yang masih belum disesuaikan dengan kondsi dari organisasi. Tujuan dari proses verifikasi ini adalah untuk mengetahui kelengkapan dari dokumen prosedur audit yang telah dibuat oleh penulis. Hasil dari proses verifikasi dokumen audit program dapat di lihat pada tabel 6.1 berikut ini.

Tabel 5.10 Verifikasi Prosedur Audit

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan			**Prosedur Audit**	
No. Kontrol	***Control Objective***	***Implementation Guidance***	**No. Prosedur**	**Check list**
11.1.2	*Physical Entry Controls*	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.	1	a, b, c
		Akses ke daerah-daerah di mana informasi rahasia diproses atau disimpan harus dibatasi untuk individu yang	2	a, b

		berwenang hanya dengan menerapkan kontrol akses yang sesuai, misalnya dengan menerapkan mekanisme otentikasi dua faktor seperti kartu akses dan PIN rahasia		
		Buku log fisik atau audit trail elektronik dari semua akses harus aman dijaga dan dipantau	1	d
		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	4	a, b, c
		Tenaga pendukung layanan dari pihak eksternal harus diberikan akses terbatas untuk mengamankan daerah atau fasilitas pengolahan informasi rahasia hanya ketika diperlukan; akses ini harus disahkan dan dipantau.	3	c

Keterangan:

- Kolom "**No Kontrol**" menunjukkann nomor *control objective* yang ada pada ISO/IEC 27002:2013 untuk klausul keamanan fisik dan lingkungan.
- Kolom "***Control Objective*"** merupakan nama dari kendali tujuan yang ada pada ISO/IEC 27002:2013
- Kolom "***Implementation Guidance*"** diisi berdasarkan ISO/IEC 27002:2013 yang sesuai dengan *control objective* yang dipakai.
- Kolom "**No. Prosedur"** merupakan penamaan untuk no prosedur yang ada pada perangkat audit yang berhubungan dengan *implementation guidance*
- Kolom "**Daftar Cek"** berisikan daftar cek yang mana saja yang telah sesuai dengan *control objective* dan *implementation guidance.*

Untuk hasil verifikasi perangkat audit yang disajikan dalam betuk tabel, lebih lengkapnya ada pada bagian Lampiran B. Berdasarkan tebel tersebut dapat ditarik kesimpulan bahwa ketujuh kontrol yang didapat dari hasil pemetaan terhadap analisa risiko telah tercantum dalam prosedur audit yang dibuat.

BAB VI
HASIL DAN PEMBAHASAN

Pada bab ini akan dijelaskan mengenai hasil yang diperoleh dari tahap penyusunan dokumen panduan audit serta proses validasi atau persetujuan dokumen panduan audit TI untuk keamanan fisik dan lingkungan ruang server STIE Perbanas Surabaya.

6.1 Hasil Penyusunan Dokumen *Audit Plan*

Seperti yang sudah dijelaskan pada tahap penyusunan dokumen *audit plan*, bahwa dokumen ini dibagi menjadi beberapa bagian yaitu Informasi Umum, Proses Audit dan Evaluasi. Pada Informasi Umum terdapat beberapa sub bagian yang sudag disusun yaitu :

1. **Tujuan**
   Dokumen Internal Audit Plan disusun untuk melakukan perencanaan terhadap audit keamanan fisik dan lingkungan teknologi informasi pada ruang server STIE Perbanas Surabaya. Adapun tujuan dari penyusunan dokumen ini adalah sebagai berikut :
   - Memberikan informasi mengenai cakupan dari sistem yang akan diaudit
   - Memberikan informasi kepada perusahaan atau organisasi mengenai pihak – pihak yang akan terlibat selama proses audit dilakukan.
   - Memberikan informasi mengenai jadwal pelaksanaan audit internal.

2. **Ruang Lingkup**
   Ruang lingkup pada dokumen *Internal Audit Plan* akan menjelaskan mengenai berbagai batasan dalam pelaksanaan proses audit untuk kemanan fisik dan lingkungan teknologi informasi pada ruang server STIE Perbanas Surabaya. Berikut ini adalah ruang lingkup dari dokumen Internal Audit Plan :

- Memahami proses bisnis Bagian TIK STIE Perbanas Surabaya selaku penanggung jawab serta pengelola ruang server yang meliputi :
  a. Pengamanan terhadap peralatan TI yang ada di ruang server
  b. Monitoring atau pemantauan kondisi keamanan area kerja
  c. Keamanan fisik dan lingkungan teknologi informasi yang diterapkan oleh Bagian TIK STIE Perbanas Surabaya secara rutin atau berkala
  d. Proses pengadaan dan pembuangan apabila barang atau aset sudah tidak dapat dipergunakan lagi
  e. Proses perawatan serta penanggulangan gangguan pada aset TI
- Melakukan identifikasi serta mengelola semua risiko yang mungkin bisa terjadi pada proses bisnis Bagian TIK STIE Perbanas Surabaya selaku penanggung jawab dan pengelola ruang server.
- Memberikan penjelasan mengenai jenis internal audit yang akan diterapkan.
- Memberikan informasi mengenai metode yang akan digunakan pada saat pelaksanaan internal audit.
- Menginformasikan peran dan tanggung jawab dari Bagian Satuan Pengawas Internal (SPI) selama proses audit berlangsung.
- Menginformasikan jadwal pelaksanaan internal audit.

3. Gambaran Sistem

Berikut ini adalah penjelasan mengenai gambaran umum terkait dengan system yang akan menjadi focus selama pelaksanaan internal audit :

Nama Organisasi	:	STIE Perbanas Surabaya
Nama Sistem	:	Keamanan fisik dan lingkungan teknologi informasi pada ruang server

Diskripsi Sistem : Keamanan fisik dan lingkungan teknologi informasi pada ruang server merupakan serangkaian upaya yang dilakukan untuk menjaga keamanan peralatan atau aset teknologi informasi yang ada pada ruang server STIE Perbanas Surabaya dari ancaman – ancaman dan juga risiko yang dapat mengganggu jalannya proses bisnis organisasi. Keamanan fisik dan lingkungan teknologi informasi yang dimaksudkan adalah meliputi tata kelola yang dapat berupa kebijakan, prosedur serta formulir yang terkait dengan aktivitas pemeliharaan seperti berikut :

Kondisi kekinian sistem :

- Memiiki prosedur pemeliharaan aset
- Memiliki prosedur monitoring dan penilaian kerusakan aset
- Memiliki kebijakan untuk pemeliharaan ruang server
- Memiliki formulir untuk check aset dan pemeliharaan aset
- Terdapat aset pelindung
- Terdapat kunci untuk kontrol akses masuk

Untuk bagian Informasi Umum yang berisikan tujuan, ruang lingkup, gambaran sistem, referensi, akronim dan singkatan, serta kontak lebih lengkap dapat dilihat pada buku produk berupa Dokumen *Audit Plan* pada halaman 4 sampai dengan halaman 6.

Untuk bagian Proses Audit berisikan beberapa sub bagian seperti berikut.

1. **Tipe Audit Internal**
   Dalam proses Audit Internal, terdapat dua tipe audit yang akan dilakukan untuk keamanan fisik dan lingkungan ruang server STIE Perbanas Surabaya. Kedua tipe Audit Internal tersebut adalah sebagai berikut :
   a. Audit Operational (kinerja)
      Tipe audit operational merupakan suatu pemeriksaan yang dilakukan untuk melihat kegiatan operational untuk keamanan fisik dan lingkungan teknologi informasi di ruang server STIE Perbanas Surabaya. Hal ini bertujuan untuk mengetahui apakah semua kegiatan operational sudah dilakukan secara efektif dan efisien, serta ekonomis.
   b. Audit Compliance (ketaatan)
      Tipe audit compliance dilakukan untuk mengetahui apakah Bagian TIK STIE Perbanas Surabaya sudah mentaati semua peraturan serta kebijakan yang telah diberlakukan terkait dengan keamanan fisik dan lingkungan teknologi informasi di ruang server STIE Perbanas Surabaya.

2. **Subjek Audit Internal**
   Berikut ini merupakan subjek area yang akan terlibat selama proses Audit Internal keamanan fisik dan lingkungan teknologi informasi di ruang server STIE Perbanas Surabaya :
   a. Bagian TIK STIE Perbanas Surabaya merupakan tempat dimana proses internal audit akan dilakukan, khususnya pada ruang server yang dimiliki.
   b. Ruang server yang terdapat pada STIE Perbanas Surabaya dinaungi oleh Bagian TIK, sehingga bagian inilah yang akan berperan penting selama proses audit internal.

c. Kepala Bagian TIK merupakan pihak yang memiliki tanggung jawab terbesar terkait dengan kondisi dari ruang server STIE Perbanas Surabaya.
d. Anggota atau Staff Bagian TIK merupakan pihak yang melaksanakan semua proses keamanan fisik dan lingkungan teknologi informasi di ruang server STIE Perbanas Surabaya.

Selain itu, terdapat informasi mengenai Peran dan Tanggung Jawab, Metode Audit Internal, serta Jadwal Kegiatan yang dapat dilihat pada buku produk Dokumen Audit Plan pada halaman 8 sampai dengan halaman 17.

Baagian terakhir adalah Evaluasi yang berisikan Strategi serta *Risk Assesment*, dimana adanya bagian ini bertujuan untuk membantu auditor dalam mengantisipasi kendala baik berupa risiko yang dapat menghambat pelaksanaan audit. Berikut adalah salah satu isi dari sub bagian Evaluasi.

1. *Risk Assesment*

a. Tujuan Manajemen Risiko
   Agar dapat melaksanakan proses audit dengan lebih baik dan untuk mengurangi kesalahan selama pelaksaan kegiatan audit, maka perlu dibuatkan sebuah rencana manajemen risiko untuk mengantisipasi kesalahan dan kesulitan yang dihadapi selama pelaksaan audit. Tujuannya adalah untuk membantu pihak auditor dalam membangun dan mengembangkan sebuah strategi yang dapat diimplementasikan untuk menghadapi berbagai macam risiko yang mungkin terjadi. Rencana manajemen risiko ini dapat dibuat dengan melihat kemungkinan risiko dan bagaimana mengelola serta mengantisipasi risiko tersebut.
b. Identifikasi Risiko Selama Proses Audit
   Berikut ini merupakan daftar risiko dalam bentuk tabel yang mungkin bisa terjadi selama proses pelaksanaan audit berlangsung.

Tabel 6.1 Identifikasi Risiko Selama Proses Audit

Risiko	Rencana Mitigasi
Proses pelaksanaan audit tidak dapat diselesaikan dalam jangka waktu yang sudah disetujui sebelumnya.	• Memantau secara terus menerus kesesuaian jadwal dengan pelaksanaan aktivitas di lapangan. • Memecah tugas dan tanggung jawab anggota tim audit. • Mempersingkat durasi aktivitas yang dirasa tidak begitu berpengaruh.
Terdapat anggota tim audit yang pergi dengan alasan urusan penting lain yang mendadak.	• Mengalokasikan 2 atau lebih sumber daya untuk aktivitas atau tugas yang dirasa penting dan berpengaruh besar dalam proses audit.
Anggota tim audit tidak memiliki kemampuan yang cukup memadai dalam melakukan audit dengan ruang lingkup atau bidang yang sudah ditentukan.	• Memberikan pelatihan dan pembekalan kemampuan kepada anggota tim audit. • Memilih anggota tim audit sesuai dengan ruang lingkup pelaksanaan audit saat ini.
Anggota tim audit tidak hadir dalam rapat sehingga tidak mengetahui perkembangan audit yang dilaksanakan.	• Menginformasikan hasil rapat melalui media telekomunikasi sehingga selalu dapat dilihat oleh semua anggota tim audit.

Risiko	Rencana Mitigasi
Pihak auditee tidak dapat memberikan informasi secara mendetail dan lengkap.	• Lebih mendetailkan kebutuhan informasi yang ingin diperoleh auditor pada saat rapat dengan auditee dan organisasi • Memberikan pengertian kepada pihak auditee dan organisasi bahwa informasi yang diberikan akan mempengaruhi hasil dari pelaksaan audit.
Kesulitan dalam menjalin komunikasi dengan pihak auditee dan organisasi	• Mengalokasikan waktu pertemuan dengan auditee dan mendiskusikannya untuk mendapat kesepakatan bersama.

Bagian evaluasi yang lebih detail dan lengkap dapat dilihat pada Dokumen *Audit Plan* pada halaman 19 sampai dengan 21.

6.2 Hasil Penyusunan Dokumen *Audit Program*

Dokumen Audit Program yang disusun penulis terdiri dari beberapa bagian yaitu bagian Informasi Umum, Penilaian Risiko, Perangkat Audit, serta Panduan Penggunaan Perangkat Audit. Berikut ini adalah salah satu isi dari dokumen Audit Program.

1. Perangkat Audit

a. Daftar Perangkat Audit

Pada bagian ini berisikan daftar dari perangkat audit yang dipergunakan untuk melakukan proses pemeriksaan pada kontrol yang sudah ditentukan di bagian *Control Objective*. Adapun kontrol yang harus diperiksa adalah :

Tabel 6.2 Daftar Perangkat Audit

No.	ID Dokumen	Nama Dokumen
1.	P.1.2	*11.1.2 Physical entry controls*
2.	P.1.4	*11.1.4 Protecting against external and environmental threats*
3.	P.1.5	*11.1.5 Working in secure areas*
4.	P.2.1	*11.2.1 Equipment sitting and protection*
5.	P.2.2	*11.2.2 Supporting Utilities*
6.	P.2.3	*11.2.3 Cabling security*
7.	P.2.4	*11.2.4 Equipment maintenance*

Berikut ini adalah salah satu contoh perangkat audit dengan ID Dokumen P.2.2 yang sudah dibuat.

STIE Perbanas
www.perbanas.ac.id

PROSEDUR AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI RUANG SERVER STIE PERBANAS SURABAYA

11.2.2 Supporting Utillities	**P.2.2**	
Peralatan harus dilindungi dari gangguan listrik dan gangguan lain yang disebabkan oleh kegagalan dari sarana pendukung.	AUDITOR *ttd* (Nama Auditor)	AUDITEE *ttd* (Nama Auditee)

TANGGAL & WAKTU :

Audit Procedure	Testing	Audit Checklist	Yes	No	Partial	Evidence
Auditor melakukan pengecekan terhadap sarana pendukung yang digunakan untuk menunjang aset yang ada di ruang server. 1. Auditor mencari dan mengumpulkan informasi serta melakukan observasi mengenai peralatan berupa sarana pendukung yang menunjang aset di raung server	**Compliance**	a. Apakah perusahaan/organisasi sudah memiliki generator pembangkit tenaga listrik yang dapat menyediakan daya listrik ketika terjadi pemadaman?				Dokumen daftar aset Foto genset
	Compliance	b. Jika ada, apakah terdapat dokumen untuk spesifikasi generator pembangkit tenaga listrik yang dimaksud?				Dokumen spesifikasi alat
	Compliance	c. Apakah perusahaan/organisasi sudah memiliki UPS (*Uninterruptible Power Supply*) untuk menjaga peralihan daya listrik ke generator ketika terjadi pemadaman?				Dokumen daftar aset Foto UPS
	Compliance	d. Jika ada, apakah terdapat dokumen untuk spesifikasi dari UPS tersebut?				Dokumen spesifikasi alat

Gambar 6.1 Contoh Perangkat Audit P.2.2

b. Formulir Pelaksanaan Tindak Lanjut
Bagian selanjutnya adalah formulir hasil tindak lanjut yang sudah dilakukan oleh pihak organisasi terhadap temuan pada pemeriksaan tertentu. Formulir ini diiskan oleh pihak organisasi dan ditandatangani oleh pelaksana tindak lanjut dan Auditor.

FORMULIR AUDIT FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI RUANG SERVER STIE PERBANAS SURABAYA	STIE Perbanas www.perbanas.ac.id
Pelaksanaan Tindak Lanjut Internal No. Program :	
Tanggal Audit : [DD-MM-YYYY]	**Nama Kontrol** : [isikan sesuai dengan nama kontrol]
Pelaksana : [isikan nama pelaksana]	
Pelaksanaan : [isikan program yang telah dilakukan oleh organisasi]	
Tanggal Penyelesaian : [DD-MM-YYYY]	
Pengesahan Pelaksana : Auditor : Kepala Bagian TIK : (……) (……) (……)	

Gambar 6.2 Formulir Pelaksanaan Tindak Lanjut

Untuk isi dari dokumen audit program yang lebih lengkap dapat dilihat pada buku produk Dokumen *Audit Program*.

6.3 Peretujuan Dokumen Panduan Audit TI

Proses persetujuan dokumen panduan audit ini dilakukan dengan penyerahan dokumen *audit plan* dan *audit program* kepada pihak organisasi untuk di-*review* setelah dilakukan perbaikan sesuai dengan saran yang diberikan ketika proses verifikasi dokumen *audit plan* dan juga *audit program*.

6.3.1 Perencanaan Proses Persetujuan

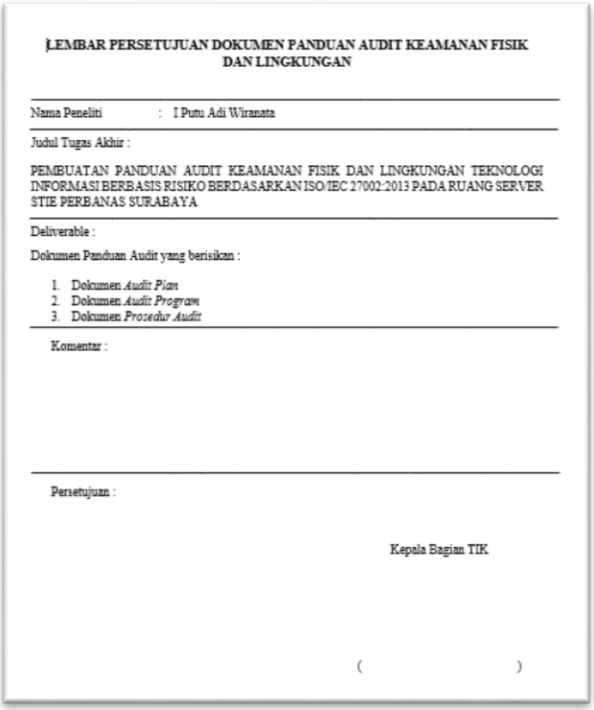
Dalam pelaksanaan, proses persetujuan atau validasi akan dilakukan dengan menggunakan metode acceptance testing kepada pihak Bagian TIK STIE Perbanas Surabaya karena bagian inilah yang diberikan tanggung jawab dalam pengelolaan ruang server milik STIE Perbanas Surabaya. Proses acceptane Testing akan dilakukan melalui media email dan juga tatap muka langsung. Berikut ini adalah perencanaan aktivitas persetujuan yang ditampilkan dalam Tabel 6.1.

Tabel 6.1 Perencanaan Persetujuan Dokumen Panduan Audit TI

Jenis Validasi	Validasi Dokumen secara langsung	
Pelaku	Kepala Bagian TIK	
Aktivitas	**No**	**Deskripsi**
	1	Peneliti memberikan dokumen *audit plan* kepada kepala Bagian TIK STIE Perbanas Surabaya untuk di review.
	2	Peneliti menerima masukan yang diberikan terkait dengan informasi auditor.
	3	Peneliti memberikan hasil dokumen audit program yang telah disusun untuk di review.
	4	Peneliti menerima masukan yang diberikan.
	5	Peneliti melakukan perbaikan pada dokumen *audit plan* dan *audit program.*
	6	Peneliti memberikan kembali dokumen *audit plan* dan *audit program.*
	7	Kepala Bagian TIK menerima dan menyetujui perbaikan yang telah dilakukan.

6.3.2 Hasil Persetujuan Panduan Audit

Secara umum hasil dari persetujuan dengan pihak Bagian TIK STIE Perbanas Surabaya terkait dengan dokumen panduan audit yang telah dibuat dapat diterima dan disetujui karena pada proses verifikasi *audit plan* dan *audit program* sudah dilakukan beberapa perubahan sesuai dengan masukan yang diberikan Kepala Bagian TIK STIE Perbanas Surabaya. Berikut ini adalah contoh lembar persetujuan atau validasi yang sudah dibuat.



LEMBAR PERSETUJUAN DOKUMEN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN

Nama Peneliti : I Putu Adi Wiranata

Judul Tugas Akhir :

PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO/IEC 27002:2013 PADA RUANG SERVER STIE PERBANAS SURABAYA

Deliverable :

Dokumen Panduan Audit yang berisikan :

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

Komentar :

Persetujuan :

Kepala Bagian TIK

( )

Gambar 6.3 Lembar Validasi

Untuk lembar persetujuan atau validasi yang sudah ditandatangani dapat dilihat pada bagian Lampiran C.

6.4 Contoh Pengisian Dokumen Prosedur Audit

Berikut ini adalah contoh pengisian dari dokumen prosedur audit yang ada dalam Audit Porgram yang dapat dilihat pada Gambar 6.4, Gambar 6.5 dan Gambar 6.6.

STIE Perbanas www.perbanas.ac.id	PROSEDUR AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI RUANG SERVER STIE PERBANAS SURABAYA		
	11.2.2 Supporting Utillities	P.2.2	
	Peralatan harus dilindungi dari gangguan listrik dan gangguan lain yang disebabkan oleh kegagalan dari sarana pendukung.	AUDITOR *ttd* (Gunasti)	AUDITEE *ttd* (Hariadi Y.)

TANGGAL & WAKTU : 8 Maret 2017, Pukul 10.00 AM

Audit Procedure	Testing	Audit Checklist	Yes	No	Partial	Evidence
Auditor melakukan pengecekan terhadap sarana pendukung yang digunakan untuk menunjang aset yang ada di ruang server. 1. Auditor mencari dan mengumpulkan informasi serta melakukan observasi mengenai peralatan berupa sarana pendukung yang menunjang aset di raung server	**Compliance**	a. Apakah perusahaan/organisasi sudah memiliki generator pembangkit tenaga listrik yang dapat menyediakan daya listrik ketika terjadi pemadaman?	√			*Generator tercatat dalam dokumen daftar aset yang dimiliki organisasi. Dokumen dan foto aset akan dilampirkan*
	Compliance	b. Jika ada, apakah terdapat dokumen untuk spesifikasi generator pembangkit tenaga listrik yang dimaksud?		√		*Dokumen spesifikasi alat tidak tersedia*
	Compliance	c. Apakah perusahaan/organisasi sudah memiliki UPS (*Uninterruptible Power Supply*) untuk menjaga peralihan daya listrik ke generator ketika terjadi pemadaman?	√			*UPS tercatat dalam dokumen daftar aset* *Dokumen daftar aset dan foto UPS akan dilampirkan*
	Compliance	d. Jika ada, apakah terdapat dokumen untuk spesifikasi dari UPS tersebut?		√		*Dokumen spesifikasi untuk UPS tidak tersedia*
	Compliance	e. Apakah organisasi sudah memiliki alat untuk menjaga kestabilan temperatur aset yang ada di ruang server?	√			*Pada ruang server terdapat 2 alat pendingin ruangan. Foto alat akan dilampirkan*
2. Auditor melakukan pengecekan terkait dengan kemampuan dari sarana pendukung daya atau tenaga listrik.	**Substantive**	a. Apakah generator pembangkit daya listrik yang dimiliki mampu mensuplay daya listrik yang dibutuhkan untuk aset di ruang server? (Hitung total daya yang dihasilkan generator dan bandingkan dengan daya yang dibutuhkan aset di ruang server)	√			*Genset menghasilkan daya yang lebih besar dari kebutuhan daya ruang server*
	Substantive	b. Apakah UPS yang dimiliki mampu menjaga dan memastikan peralihat daya dari aset di ruang server? (Hitung waktu yang dibutuhkan untuk mengaktifkan generator dan bandingkan dengan berapa lama UPS dapat mensuplay daya)				*Untuk menghidupkan genset dibutuhkan waktu 10 menit, dan UPS mampu mensuplay daya selama 60 menit*

Gambar 6.4 Contoh Pengisian Prosedur Audit

3. Auditor melakukan pengecekan terkait dengan perawatan untuk sarana pendukung yang ada.	**Compliance**	a. Apakah terdapat ketentuaan atau prosedur untuk perawatan rutin terhadap generator pembangkit tenaga listrik?		√		*Tidak tersedia prosedur perawatan rutin untuk genset*
	Substantive	b. Jika ada, apakah generator pembangkit daya listrik sudah dirawat secara teratur atau sesuai dengan prosedur yang ada? (Periksa dokumen log perawatan)			√	*Perawatan hanya dilakukan ketika genset mengalami kegagalan fungsi*
	Compliance	c. Apakah terdapat ketentuaan atau prosedur untuk perawatan rutin terhadap UPS yang dimiliki?	√			*Tersedia log perawatan untuk aset dan akan dilampirkan*
	Substantive	d. Jika ada, apakah UPS sudah dirawat secara teratur atau sesuai dengan prosedur yang ada? (Periksa dokumen log perawatan)	√			*Log perawatan aset akan dilampirkan*
4. Auditor melakukan pemeriksaan untuk perangkat penanda kegagalan fungsi sarana penduung	**Compliance**	a. Apakah terdapat penanda semacam alarm baik berupa suara maupun cahaya lampu yang mengindikasikan kegagalan fungsi sarana pendukung?	√			*Terdapat indicator lampu Foto indicator lampu akan dilampirkan*
	Substantive	b. Jika ada, periksa apakah penanda yang dimaksud masih berfungsi dengan baik?	√			*Foto indicator lampu akan dilampirkan*
5. Auditor mengumpulkan informasi dan melakukan observasi terkait dengan jalur sarana pendukung	**Compliance**	a. Apakah ruang server STIE Perbanas Surabaya sudah memiliki jalur sumber listrik, telekomunikasi, air, dan pertukaran udara yang baik? (Lakukan pengecekan secara fisik terhadap aliran listrik, air, dan ventilasi udara)	√			*Terdapat denah alur sumber listrik dan air. Foto terkait akan dilampirkan*
	Substantive	b. Apakah jalur dari aliran listrik, air, dan telekomunikasi sudah dipisahkan? (Lakukan pemeriksaan secara fisik)	√			*Foto jalur aliran listrikair, dan telekomunikasi akan dilampirkan*

Gambar 6.5 Contoh Pengisian Prosedur Audit

LAPORAN PEMERIKSAAN
No Temuan : TP.2.2

Tanggal Pemeriksaan : 8 Maret 2017 | **Auditor :** Gunasti | **Auditee :** Hariadi Y.

Klausul : ***11.2.2 Supporting Utillities***

Risiko Terkait :
Kegagalan Daya yang disebabkan oleh kegagalan fungsi dari genset

Kesimpulan :
Secara keseluruhan, implementasi dari kontrol Supporting Utilities telah dilakukan dengan cukup baik. Beberapa prosedur untuk perawatan telah ada, namun masih terdapat sarana pendukung yang tidak secara rutin dirawat padahal memiliki peran yang cukup signifikan terhadap aset yang ada pada ruang server.

Risiko	Detect	RPN	Level
R - 14	5	140	high

Usulan Tindak Lanjut :
Kebijakan atau prosedur untuk perawatan terhadap sarana pendukung perlu diterapkan sepenuhnya terhadap sarana yang memegang peran signifikan seperti pendukung daya cadangan. Dan pelaksanaan dari perawatan harus mengacu pada prosedur yang sudah ada.

Batas Penyelesaian Perbaikan :
8 Juni 2017

Penanggung Jawab :
Anton

Pengesahan :

Auditee	Auditor
(Hariyadi Yutanto)	(Gunasti)

Gambar 6.6 Contoh Pengisian Laporan Pemeriksaan

Halaman ini sengaja dikosongkan

BAB VII
KESIMPULAN DAN SARAN

Bab ini berisikan penjelasan mengenai kesimpulan dari hasil penelitian yang dilakukan oleh penulis serta saran yang akan bermanfaat untuk perbaikan dalam penelitian selaanjutnya dengan topik yang terkait.

7.1 Kesimpulan

Dari proses dan juga tahapan yang telah dilalui dalam pengerjaan tugas akhir ini, maka dapat diambil beberapa kesimpulan yang dapat menjawab rumusan masalah yang telah ditentukan, yaitu :

1. Berdasarkan hasil identifikasi risiko yang telah dilakukan didapatkan 30 risiko yang dikembangkan dari identifikasi ancaman dan kerentanan terhadap setiap aset di ruang server. Semua risiko yang berhasil diidentifikasi termasuk ke dalam kontrol keamanan fisik dan lingkungan.
2. Dari hasil pemetaan risiko dengan kontrol ISO/IEC 27002:2013 klausul 11 yaitu Keamanan Fisik dan Lingkungan, didapatkan bahwa terdapat 7 kontrol yang digunakan dalam pembuatan perangkat audit, diantaranya ;
   a. *11.1.2 Physical entry controls*
   b. *11.1.4 Protecting against external and environmental threats*
   c. *11.1.5 Working in secure areas*
   d. *11.2.1 Equipment sitting and protection*
   e. *11.2.2 Supporting Utilities*
   f. *11.2.2 Supporting Utilities*
   g. *11.2.4 Equipment maintenance*
3. Pada dokumen *Audit Plan*, terdapat jadwal audit yang mengadopsi proses audit pada ISO 19011 yang terdiri dari

3 aktivitas utama yakni *Preparation*, *Execution*, dan *Closing*. Untuk aktivitas Preparation terdiri dari 2 sub aktivitas utama yaitu *Initiation* serta *Planning* dimana hal inilah yang menjadi fokus dalam pengerjaan tugas akhir ini.

4. Dalam dokumen *Audit Program* terdapat 7 perangkat audit yang berisikan 28 *Prosedur Audit* serta 81 *Checklist Audit* yang mengacu pada 7 *control objective* ISO/IEC 27002:2013 klausul 11. Pada dokumen Audit Program juga disertakan panduan untuk penggunaan semua perangkat audit yang telah dibuat.

7.2 Saran

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

1. Pada penelitian ini, identifikasi risiko dilakukan dengan melihat ancaman dan kerenatanan dari setiap aset terlebih dahulu untuk mendapatkan risiko dari setiap asetnya. Peneliti tidak menggunakan referensi mengenai identifikasi risiko yang sudah pernah dilakukan pada Bagian TIK STIE Perbanas Surabaya. Penelitian selanjutnya dapat memadukan hasil identifikasi risiko dengan mengacu dari hasil identifikasi risiko yang sudah pernah dilakukan, sehingga proses ini tidak akan memakan waktu yang lama dan mengahasilkan identifikasi yang lebih baik.
2. Dalam pembuatan perangkat audit pada penelitian ini masih menggunakan acuan penelitian serupa sebelumnya yang juga menghasilkan perangkat audit. Untuk selanjutnya, format perangkat audit yang dibuat sebaiknya juga menyesuaikan dengan format pendokumentasian terkait dengan proses audit yang diterapkan oleh organisasi.

DAFTAR PUSTAKA

[1] K. I. Anasthasia, "*Teknologi Informasi Dalam Organisasi*," Jimbaran, 2011.

[2] ISO/IEC. 2005. *Information Technology-Security Techniques-Code of Practice for Information Security Management ISO/IEC 17799 (27002):2005*. Switzerland.

[3] Tim Direktorat Keamanan Informasi, *Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik*, Kominfo, 2011.

[4] Stephen Christian, *Pembuatan Panduan Audit Kemanan Fisik dan Lingkungan Teknologi Informasi Berbasis Risiko Berdasarkan ISO/IEC 27002:2013 Pada Direktorat Sistem Informasi Universitas Airlangga*, Surabaya: ITS, 2015.

[5] 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.

[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] Whittington,O.Ray dan Kurt Pany (2012). *Principles of Auditing, and Other Assurance*

Services, 18th Edition, Mc-Graw-Hill, New York, NY.

[8] Arens, Alvin A, Elder, Randal J, Mark S. Beasley (2010). A*uditing and Assurance Service, An Integrated Approach, 19tn Edition*, Prentice Hall, Englewood Clifts, New Jersey.

[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] Dr. rer. nat. I Made Wiryana, S.Kom, S.Si, MAppSc dkk, *Bakuan Audit Keamanan Informasi Kemenpora*, 2012.

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

[13] ISO, *ISO 19011: Guidelines for Auditing Management*, Switzerland: ISO, 2011.

[14] Rohmani, Asih. (2014). "*Proteksi Aset Informasi*". Semarang, Indonesia : Udinus Repository.

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

[16] Fisk, E.R.1997. *Construction Projectb Administration Fifth Edition*.Prentice Hall. New Jersey.

[17] Duffield, C & Trigunarsyah, B. 1999. *Project Management-Conception to Completion*. Engineering Educatio Australia. (EEA). Australia.

[18] Blokdijk, Gerrard. (2008). *IT Risk Management Guide.* Australia. Emereo Publishing

[19] "ISO 31000 Risk Management.pdf".

[20] "Control Objective ISO 27001.pdf".

[21] T.M. Tuanankotta, Audit Berbasis ISA, Jakarta:Salemba Embat, 2013

(halaman ini sengaja dikosongkan)

BIODATA PENULIS

Penulis bernama lengkap I Putu Adi Wiranata, namun terbiasa dipanggil Krishna. Penulis lahir di Sembung Meranggi, pada 27 Maret 1994 dan merupakan anak pertama dari dua bersaudara. Penulis telah menempuh jenjang pendidikan formal di SD Negeri No. 1 Sembung Gede, SMP Negeri 2 Kerambitan, dan SMA Negeri 1 Tabanan.

Setelah lulus dari SMA pada tahun 2012, penulis diterima di Jurusan Sistem Informasi, Institut Teknologi Sepuluh Nopember Surabaya melalui jalur SNMPTN Undangan dan terdaftar dengan NRP 52 12 100 033. Selama masa perkuliahan di ITS, penulis pernah terlibat dan aktif di organisasi kerohanian Hindu (TPKH-ITS) selama 2 tahun kepengurusan. Penulis juga pernah menjalani masa Kerja Praktik di PT. INKA (Industri Kereta Api) Madiun dan ditempatkan pada divisi IT selama kurang lebih satu setengah bulan pada tahun 2015.

Pada pengerjaan Tugas Akhir di Jurusan Sistem Informasi ITS, penulis mengambil bidang minat Manajemen Sistem Informasi dengan topik Manajemen Risiko TI dan Audit TI, yakni Pembuatan Panduan Audit Keamanan Fisik dan Lingkungan Teknologi Informasi Berbasis Risiko Berdasarkan ISO/IEC 27002:2013 Pada Ruang Server STIE Perbanas Surabaya. Untuk kepentingan penelitian atau yang lainnya, penulis dapat dihubungi melalui email di adi.wiranata33@gmail.com.

(halaman ini sengaja dikosongkan)

LAMPIRAN A
HASIL WAWANCARA

Pada bagian Lampiran A ini berisikan daftar transkrip hasil wawancara dengan pihak STIE Perbanas Surabaya yang telah dilakukan oleh penulis selama pengerjaan tugas akhir.

Tanggal Wawancara : 20 Mei 2016
Media : Whats App
Jabatan Narasumber : Kepala Bagian TIK
Tujuan Wawancara : Aset TI di ruang server

Tabel A.1 Transkirp Wawancara Terkait Aset TI di Ruang Server

Pertanyaan	Jawaban
Selamat siang mas, nanti saya bisa menemui mas dimana ya? Terima kasih	Siang dek. Kalau senin aja gimana dek, di kampus 2
Kalau siang ini gak bisa mas? Mau tanya – tanya sedikit saja sih	Saya sedang di luar dek. Mungkin bisa diskusi di wad ulu dek. Kira – kira apa yang mau dikerjakan

A-2

Pertanyaan	Jawaban
Oalah, iya mas. Maaf mengganggu	Gimana – gimana dek
Begini mas, saya mengambil topik pembuatan panduan audit untuk keamanan fisik dan lingkungan ruang server mas. Panduan audit itu nanti ada audit plan sama audit program. Pembuatan audit program ini berbasis risiko untuk setiap aset yang ada di ruang server mas. Untuk saat ini saya membutuhkan informasi terkait aset – aset apa saja yang disimpan di ruang server mas.	Di ruangan server terdapat 2 rackmount. 1 rack dikhususkan untuk perangkat jaringan seperti router, switch, modem.
Apakah itu ada dokumen asetnya mas? Dokumen yang berisikan daftar aset di ruangan tersebut maksud saya	Untuk yang baru ini masih belum ter-update soalnya habis kebakaran, untuk inventaris ada di unit umum.
Berarti ada dokumennya, tapi untuk yang dulu ya mas?	Iya
Apa jauh berbeda mas dengan yang sekarang? Daftar asetnya maksud saya	Iya, jauh dek. Banyak yang dirombak. Tapi tetep basic nya pakai mikrotik semua. Tapi dari segi tatanan infrastruktur dirombak.
Saya ingin melihat langsung sebenarnya mas, dan sekalian membuat dokumen daftar aset yang ada di ruang tersebut. Apakah memungkinkan mas?	Daftar aset di ruangan server gak ada dek. Habis dimakan si jago merah.
Nah itu mas, maunya sekalian saya bikinkan	Ok dek.

Pertanyaan	Jawaban
Tapi saya perlu liat dokumen aset yang lama mas, untuk referensi formatnya. Biar tidak jauh berbeda dengan standar yang diapakai di sana.	Formatnya tabel biasa dek. Cuman ditempelkan di dinding.
Oke mas. Senin nanti kira – kira saya bisa menemui mas tidak?	Iya, bisa dek. Jam 12 ya dek. Tapi di kampus 2.

Kesimpulan Wawancara Tabel A.1 :
Pada ruang server milik STIE Perbanas yang baru secara umum terdapat 2 rackmount. 1 rack dikhususkan untuk perangkat jaringan seperti router, switch, modem. Untuk lebih detailnya, narasumber tidak bisa menyebutkan dan diperlukan observasi secara langsung ke ruangan server.

Tanggal Wawancara : 12 Oktober 2016
Media : Tatap muka
Jabatan Narasumber : Kepala Bagian TIK
Tujuan Wawancara : Kondisi ruang server

Tabel A.2 Transkrip Wawancara Terkait Kondisi Ruang Server

Pertanyaan	Jawaban
Siang mas. Jadi gini mas, saya ingin menanyakan terkait dengan ruang server nya mas.	Iya siang dek, mau tanya tentang apanya ?
Jadi yang bertanggung jawab untuk ruang server nya itu siapa mas?	Untuk tanggung jawab sebenernya itu bersama bagian umum dek. Tapi untuk pengelolaan aset dan

Pertanyaan	Jawaban
	perlindungannya diberikan ke Bagian TIK.
Jadi pihak umum juga punya akses ke ruang server nya mas?	Punya, tapi hanya beberapa orang tertentu yang sudah disetujui dek. Dan orng-orang itu sudah punya kunci ruangan nya.
Pengamanan akses masuknya kunci itu saja mas.	Iya, untuk sekarang ini baru kunci saja. Soalnya ini kan habis kebakaran dan baru pindahan juga ke ruangan ini.
Oalah, kok bisa kebakaran mas? Memangnya tidak ada smoke detector atau alarm gitu?	Waktu itu belum ada dek. Cuma ada tabung pemadam saja, dan itu juga bukan khusus buat ruang server sebenernya.
Jadi ini semua peralatannya baru berarti mas?	Iya, soalnya yang dulu habis dimakan si jago merah.
Oalah, kalau untuk perawatan peralatan yang ada di ruangan itu gimana?	Ya perawatannya juga jadi tanggung jawab Bagian TIK dek.
Prosedur atau kebijakannya ada itu mas?	Ada dek
Berarti setiap ada perawatan aset gitu dicatat mas?	Iya dicatat dek. Ada laporan berita acaranya juga dulu.
Terus sekarang gimana mas?	Sekarang masih belum ada dek, soalnya habis dimakan si jago merah. Tapi mungkin dibagian umum atau administrasi gitu masih menyimpan yang dulu. Kalau di TIK sendiri sekarang masih belum ada.

Pertanyaan	Jawaban
Untuk daftar aset yang ada di ruangan gitu ada mas?	Kalau sekarang ini belum ada dek, dulu ada sebelum kebakaran.
Kalau saya ingin melihat ruangan servernya bisa gak mas? Saya ingin melihat langsung aset yang ada di sana apa saja mas, mau saya catat sekalian.	Oiya bisa dek. Saya ambilkan kuncinya dulu.
Untuk standar keamanan yang diapakai sendiri itu ada tidak mas?	Maksudnya dek?
Kayak standar keamanan informasi dari ISO, atau COBIT gitu mas.	Ohh, kalau untuk keamanan informasi sih kita ngacu ISO dek. Cuman ya penerapannya masih secara umum saja.
Oalah, kalau untuk keamanan fisik dan lingkungan itu bagaimana mas?	Kalau itu kita masih secara umum juga dek. Pengamanan yang standar secara umumlah, yang sering dipakai untuk mengamankan ruang tertentu kayak ruang server.
Oalah, ini kalau nanti saya mengacu ke standar ISO/IEC 27002:2013 bisa gak mas?	Iya gpp dek, sekalian kita mau perbaiki pengamanan nya juga. Kan baru habis kebakaran juga.
Kalau audit gitu pernah dilakukan tidak mas?	Itu pasti dek. Dari yayasan selalu melakukan audit setiap awal semester.
Itu bulan apa mas biasanya? Dan berapa lama pelaksanaan audit nya?	Bulan maret sama agustus kalau tidak salah. Itu paling Cuma seminggu biasanya dek.
Itu yang di audit terkait dengan apa biasanya mas?	Biasanya lebih ke arah ketersediaan dari layanan seperti down time server gitu dek.

Pertanyaan	Jawaban
Baiklah mas. Untuk saat ini kayaknya itu aja yang saya tanyakan. Nanti kalau ada perlu lagi saya hubungi mas.	Iya dek, nanti WA saya saja kalau mau ketemu.

Kesimpulan Wawancara Tabel A.2 :
Untuk pengelolaan ruang server termasuk juga semua aset yang ada di dalamnya secara garis besar menjadi tanggung jawab dari Bagian TIK STIE Perbanas Surabaya. Namun dalam pelaksanaan pengelolaannya masih harus berkoordinasi dengan Bagian Umum. Dari segi pengamanan untuk akses ruangan masih menggunakan kunci yang hanya dimiliki oleh orang tertentu. Untuk pengelolaan aset yang ada di ruangan sendiri sudah memiliki prosedur tertulis sehingga semua kegiatan perawatan, pengadaan ataupun pembuanga aset sudah terdokumentasi. Untuk standar keamanan yang digunakan, secara umum mengacu pada ISO, namun penerapannya tidak dilakukan secara spesifik atau menyeluruh.

Tanggal Wawancara : 8 Desember 2016
Media : Whats App
Jabatan Narasumber : Kepala Bagian TIK
Tujuan Wawancara : Analisa dan Penilaian Risiko

Tabel A.3 Transkrip Wawancara Terkait Analisa & Penilaian Risiko

Pertanyaan	Jawaban
Selamat pagi mas, mohon maaf menggangu. Saya bisa minta waktunya sebentar tidak mas? Ada beberapa hal yang ingin	Pagi. Ya dek

Pertanyaan	Jawaban
saya tanyakan untuk tugas akhir saya.	
Terima kasih mas. Mas pernah menggunakan metode FMEA untuk analisa risiko tidak mas? Soalnya saya perlu penilaian risiko yang sudah saya analisa dari pihak Perbanas nya mas.	Belum pernah mas
Kalau begitu untuk penialain risiko nya saya bantu ya mas, nanti saya kirim untuk mas review. Bagaimana mas?	Iya gitu aja dek
Baik mas, terima kasih banyak. Maaf mengganggu mas.	Siap

Kesimpulan Wawancara Tabel A.3 :
Untuk analisa dan penilaian risiko penulis dibantu oleh Kepala Bagian TIK STIE Perbanas sehingga hasil dari analisa dan penilaian yang dilakukan dapat dipertanggung jawabkan karena sudah disetujui oleh pihak studi kasus sendiri.

Tanggal Wawancara : 13 Desember 2016
Media : Whats App
Jabatan Narasumber : Kepala Bagian TIK
Tujuan Wawancara : Analisa dan Penilaian Risiko

Tabel A.4 Transkrip Wawancara Terkait Analisa & Penilaian Risiko

Pertanyaan	Jawaban
Selamat sore mas. Maaf mengganggu. Saya sudah kirim email yang berisikan hasil identifikasi risiko dan penilaiannya tadi mas, mohon di cek ya mas. Terima kasih	Sore. Oke.
Bagaimana jadinya mas? Apa ada yang perlu saya perbaiki atau tambahkan lagi?	Sudah bagus itu dek. Kalau menurut saya sih sudah cukup.
Baik mas kalau begitu. Terima kasih banyak.	Oke, sama – sama.

Kesimpulan Wawancara Tabel A.4 :
Analisa dan penilaian risiko yang sudah dilakukan oleh penulis sebelumnya telah disetujui langsung oleh Kepala Bagian TIK STIE Perbanas Surabaya.

Tanggal Wawancara : 15 Desember 2016
Media : Tatap muka
Jabatan Narasumber : Kepala Bagian TIK
Tujuan Wawancara : Verifikasi Dokumen Audit Plan

Tabel A.5 Transkrip Wawancara Terkait Verifikasi Dokumen Audit Plan

Pertanyaan	Jawaban
Selamat pagi mas. Ini dokumen audit plan yang saya buat. Tolong di review, barang kali ada yang perlu diperbaiki atau ditambahkan mas	Oh ini ya hasilnya.
Iya mas, tapi ini baru audit plan nya saja.	Saya baca dulu sekilas ya dek. Jadi ini nanti proses auditnya ya dek.
Iya mas, disitu juga ada penjadwalannya. Saya sesuaikan sama informasi yang mas berikan terkait dengan jadwal audit di sini.	Oh iya dek. Sudah bagus ini saya lihat. Ini ada daftar aktivitasnya juga ya. Ini nanti sampai melakukan auditnya dek?
Enggak mas, saya cuma membuat panduan untuk pelaksanaan audit mas. Jadi nanti bisa dipakai acuan kalau malu mengaudit terkait keamanan fisik dan lingkungan ruang server nya.	Oh iya-iya. Jadi ini yang dipakai auditornya gitu ya. Ini SPI ini diganti saja, soalnya yang melakukan pemeriksaan atau audit di sini itu PPM namanya dek. Pusat Penjaminan Mutu kalau di sini.

Pertanyaan	Jawaban
Oh iya mas. Saya itu lihat referensi tugas akhir senior, saya kira namanya juga sama kalau disni. Nanti saya ganti kalau begitu.	Iya dek diganti aja.
Kalau untuk lama pelaksanaan auditnya bagaimana mas?	Kayaknya sudah bagus. Kan ini masih perencanaannya ya. Jadi tidak masalah menurut saya.
Baiklah mas. Jadi ada yang perlu diperbaiki lagi tidak mas?	Kayak nya sih itu aja dek.
Baik mas, terima kasih banyak kalau begitu.	Iya, sama – sama dek.

Kesimpulan Wawancara Tabel A.5 :
Secara umum, Kepala Bagian TIK STIE Perbanas Surabaya sudah menerima hasil berupa Dokumen Audit Plan yang telah dibuat dengan sedikit perbaikan pada bagian Informasi umum terkait pelaksana dari proses audit yang sebelumnya adalah SPI (Satuan Pengawas Internal) diganti menjadi PPM (Pusat Penjaminan Mutu) yang merupakan pihak yang bertanggung jawab dalam melaksanakan pemeriksaan di instansi terkait.

Tanggal Wawancara : 30 Desember 2016
Media : Tatap muka
Jabatan Narasumber : Kepala Bagian TIK
Tujuan Wawancara : Verifikasi Dokumen Audit Program

Tabel A.6 Transkrip Wawancara Terkait Verifikasi Dokumen Audit Program

Pertanyaan	Jawaban
Selamat pagi mas. Ini dokumen audit program yang sudah saya buat mas. Sama dokumen audit plan yang sudah saya perbaiki juga.	Oh iya dek. Saya baca yang audir porgam saja ya. Yang kemarin kayaknya gak ada tambahan lagi kalau dari saya.
Iya mas.	Ini prosedur ini buat ngecek nya ya dek? Pas audit itu.
Iya mas, itu checklist untuk prosedur yang di cek. Jadi prosedur itu dari pemetaan kontrol dari hasil analisa risiko kemarin. Itu ada 7 kontrol yang dibuatkan prosedur jadinya.	Oh iya. Ini sudah bagus sepertinya. Sudah semua berarti ya ini ada di check list nya?
Iya, sudah semua itu mas. Tapi Cuma 7 kontrol. Kalau di ISO kan ada 15 kontrol kalau tidak salah untuk yang keamanan fisik dan lingkungan.	Iya, segini aja sudah banyak kayaknya dek.

Pertanyaan	Jawaban
Iya mas, kalau mungkin mau dibaca – baca dulu lagi silahkan. Nanti kalau ada yang perlu diperbaiki atau ditambahkan tolong kabarin saya secepatnya mas.	Iya dek, ini saya bawa dulu ya.
Sekalian ini mas, saya butuh validasi untuk dokumen yang sudah saya buat, untuk keperluan di tugas akhir.	Oh iya dek. Taruh sini saja dulu. Nanti kalau sudah selesai saya baca saya kabarin lagi. Sekalian saya validasi semuanya ini.
Baik mas, terima kasih banyak.	Iya, sama – sama dek.

Kesimpulan Wawancara Tabel A.6 :
Kepala Bagian TIK STIE Perbanas Surabaya telah menerima dan menyetujui Dokumen Audit Program yang sudah dibuat penulis. Kepala Bagian TIK juga telah menandatangani lembar validasi sebagai bukti bahwa dokumen telah sah dan disetujui dan siap untuk digunakan.

LAMPIRAN B
VERIFIKASI PROSEDUR AUDIT

Tabel B.1 Verifikasi Prosedur Audit P.1.2

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan			**Prosedur Audit**	
No. Kontrol	***Control Objective***	***Implementation Guidance***	**No. Prosedur**	**Check list**
11.1.2	*Physical Entry Controls*	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.	1	a, b, c
		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 mekanisme otentikasi	2	a, b

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan			Prosedur Audit	
No. Kontrol	***Control Objective***	***Implementation Guidance***	**No. Prosedur**	**Check list**
		dua faktor seperti kartu akses dan PIN rahasia		
		Buku log fisik atau audit trail elektronik dari semua akses harus aman dijaga dan dipantau	1	d
		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	4	a, b, c
		Tenaga pendukung layanan dari pihak eksternal harus diberikan akses terbatas untuk mengamankan daerah atau fasilitas pengolahan informasi rahasia hanya ketika	3	c

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan			Prosedur Audit	
No. Kontrol	***Control Objective***	***Implementation Guidance***	**No. Prosedur**	**Check list**
		diperlukan; akses ini harus disahkan dan dipantau.		

Tabel B.2 Verifikasi Prosedur Audit P.1.4

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan			Prosedur Audit	
No. Kontrol	***Control Objective***	***Implementation Guidance***	**No. Prosedur**	**Check list**
11.1.4	*Protecting against external and environmental threats*	Saran spesialis harus diperoleh mengenai cara dalam menghindari kerusakan akibat kebakaran, banjir, gempa bumi, ledakan, kerusuhan sipil serta bentuk dari bencana alam lainnya.	1	a, b, c
			2	a, b
			3	a, b, c, dan d

Tabel B.3 Verifikasi Prosedur Audit P.1.5

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan			**Prosedur Audit**	
No. Kontrol	***Control Objective***	***Implementation Guidance***	**No. Prosedur**	**Check list**
11.1.5	*Working in Secure Areas*	Personel harus memeiliki kesadaran akan kegiatan yang dilakukan dalam daerah yang aman	1	a, b,
		Kegiatan yang dilakukan tanpa pengawasan pada daerah yang diamankan harus dihindari baik untuk alasan keamanan maupun terkait pencegahan peluang untuk aktivitas yang membahayakan	1	c
			2	a, b
		Area aman yang kosong harus secara fisik terkunci dan diperiksa secara berkala.	3	a, b, c
		Pengambilan gambar, video, audio atau perekaman dengan alat lainnya, seperti kamera pada perangkan mobile seharusnya tidak diperbolehkan kecuali sudah mendapatkan izin.	4	a, b

Tabel B.4 Verifikasi Prosedur Audit P.2.1

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan			**Prosedur Audit**	
No. Kontrol	***Control Objective***	***Implementation Guidance***	**No. Prosedur**	**Check list**
11.2.1	*Equipment Siting and Protection*	Peralatan harus diatur peletakkannya untuk meminimalkan akses yang tidak berkepentingan ke daerah kerja.	1	b, c
		Fasilitas pengoolahan informasi yang memproses data sensitive harus diposisikan secara hati – hati untuk mengurangi risiko informasi dilihat oleh orang yang tidak berwenang selama penggunaannya.	2	a, b
		Fasilitas penyimpanan harus diamankan untuk menghindari akses yang tidak sah.	1	d
		Kontrol harus diadopsi untuk meminimalkan risiko potensial ancaman secara fisik dan lingkungan misalnya pencurian, kebakaran, bahan peledak, asap, air (atau	2	a, b

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan			Prosedur Audit	
No. Kontrol	***Control Objective***	***Implementation Guidance***	**No. Prosedur**	**Check list**
		kegagalan pasokan air), debu, getaran, efek kimia, gangguan pasokan listrik, gangguan komunikasi, radiasi elektromagnetik dan vandalism.		
		Pedoman untuk makan, minum, dan merokok di dekat fasilitas pengolahan informasi harus diterapkan.	3	b, c
		Kondisi lingkungan, seperti suhu dan kelembaban harus dipantau untuk kondisi yang dapat mempengaruhi pengoprasian dasilitas pengolahan informasi.	3	d
		Perlindungan dari petir harus diterapkan pada semua bangunan dan filter proteksi petir harus dihubungkan ke semua pemasok daya yang masuk dan jaringan komunikasi.	2	c, d
		Penggunaan metode perlindungan khusus, seperti membrane keyboard harus	4	a, b

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan			Prosedur Audit	
No. Kontrol	***Control Objective***	***Implementation Guidance***	**No. Prosedur**	**Check list**
		dipertimbangkan untuk peralatan di lingkungan industry.		
		Peralatan pengolahan informasi rahasia harus dilindungi untuk meminimalkan risiko kebocoran informasi karena emanasi elektromagenetik.		

Tabel B.5 Verifikasi Prosedur Audit P.2.2

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan			Prosedur Audit	
No. Kontrol	***Control Objective***	***Implementation Guidance***	**No. Prosedur**	**Check list**
11.2.2	*Supporting Utilities*	Penyesuaian dengan spesifikasi dari pabrik peralatan dan persyaratan hokum local.	1	a, b, c
		Penilaian secara teratur untuk kapasitasnya dalam memenuhi pertumbuhan bisnis dan	2	a, b

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan			Prosedur Audit	
No. Kontrol	***Control Objective***	***Implementation Guidance***	**No. Prosedur**	**Check list**
		interaksi fungsi yang tepat		
		Pemeriksaan dan pengujian secara teratur untuk memastikan fungsi yang tepat	3	a, b, c, dan d
		Jika perlu, sediakan alarm untuk mendeteksi malfungsi	4	a, b
		Jika perlu, sediakan beberapa feed routing fisik yang beragam	3	c

Tabel B.6 Verifikasi Prosedur Audit P.2.3

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan			Prosedur Audit	
No. Kontrol	***Control Objective***	***Implementation Guidance***	**No. Prosedur**	**Check list**
11.2.3	*Cabling Security*	Kabel daya dan telekomunikasi ke fasilitas pengolahan informasi harus berada di bawah tanah jika memungkinkan, atau dengan pemberian perlindungan alternatif yang memadai.	1	a

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan			Prosedur Audit	
No. Kontrol	***Control Objective***	***Implementation Guidance***	**No. Prosedur**	**Check list**
		Kabel daya harus dipisahkan dengan kabel komunikasi untuk mencegah gangguan.	1	b
		Kontrol lebih lanjut untuk system yang kritis dan sensitive harus mempertimbangkan : 1. Instalasi saluran lapis baja dan mengunci ruangan atau kotak pada titik pemeriksaan dan pemutusan 2. Menggunakan perlindungan elektromagnetik untuk melindungi kabel. 3. Inisiasi pembersihan teknis dan pemeriksaan fisik untuk perangkat yang tidak sah yang melekat pada kabel 4. Akses dikenadalikan utuk patch panel dan ruang kabel	2	a, b, c

Tabel B.7 Verifikasi Prosedur Audit P.2.4

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan			**Prosedur Audit**	
No. Kontrol	***Control Objective***	***Implementation Guidance***	**No. Prosedur**	**Check list**
11.2.4	*Equipment Maintenance*	Peralatan harus dipelihara sesuai dengan spesifiskasi dan interval sevice yang dianjurkan oleh pemasok	1	a, b
		Hanya personil pemeliharaan yang berwenang yang boleh melakukan perbaikan dan perawatan peralatan.	2	a, b
		Catatan mengenai perkiraan kesalahan atau kesalahan actual, dan semua pemeliharaan preventif dan korektif harus disimpan	3	a, b, c
		Pengendalian yang tepat harus dilaksanakan bila peralatan dijadwalkan untuk pemeliharaan dengan mempertimbangkan apakah perawatan ini dilakukan oleh personel internal atau eksternal; bila perlu informasi	4	a, b

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan			Prosedur Audit	
No. Kontrol	***Control Objective***	***Implementation Guidance***	**No. Prosedur**	**Check list**
		rahasia harus dibersihkan dari peralatan atau personil pemeliharaan harus jelas dan bersih.		
		Semua persyaratan perawatan yang dikenakan oleh kebijakan asuransi harus dipenuhi	5	a, b
		Sebelum peralatan diletakkan kembali pada tempat semula setelah perawatan, harus dilakukan pemeriksaan untuk memastikan bahwa peralatan tersebut tidak dirusak atau mengalami kegagalan fungsi..	6	a

(halaman ini sengaja dikosongkan)

LAMPIRAN C
PERSETUJUAN DOKUMEN PANDUAN AUDIT TI

LEMBAR PERSETUJUAN DOKUMEN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN

Nama Peneliti : I Putu Adi Wiranata

Judul Tugas Akhir :

PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO/IEC 27002:2013 PADA RUANG SERVER STIE PERBANAS SURABAYA

Deliverable :

Dokumen Panduan Audit yang berisikan :

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

Komentar :

Persetujuan :

Kepala Bagian TIK

(Hariyadi Yulianto, S.Kom., M.Kom)

Gambar C.1 Hasil Validasi Dokumen Panduan Audit TI

(halamam ini sengaja dikosongkan)