TUGAS AKHIR – KS141501

PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO/IEC 27002 : 2013 PADA IS-NET JURUSAN SISTEM INFOMASI ITS

DESIGNING INFORMATION TECHNOLOGY PHYSICAL AND ENVIRONMENTAL SECURITY RISK BASED AUDIT GUIDELINE BASED ON ISO/IEC 27002 :2013 IN IS-NET DEPARTEMENT INFORMATION SYSTEM ITS

SALMAN AL FARISI
NRP 5209100058

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

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2017

TUGAS AKHIR – KS141501

PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO/IEC 27002 : 2013 PADA IS-NET JURUSAN SISTEM INFOMASI ITS

SALMAN AL FARISI
NRP 5209100058

Dosen Pembimbing

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

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2017

FINAL PROJECT – KS 141501

DESIGNING INFORMATION TECHNOLOGY PHYSICAL AND ENVIRONMENTAL SECURITY RISK BASED AUDIT GUIDELINE BASED ON ISO/IEC 27002 :2013 IN IS-NET DEPARTEMENT INFORMATION SYSTEM ITS

SALMAN AL FARISI
NRP 5209100058

Supervisor

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

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

PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO/IEC 27002 : 2013 PADA IS-NET JURUSAN SISTEM INFOMASI ITS

TUGAS AKHIR

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

Oleh:

SALMAN AL FARISI
5209 100 058

Surabaya, Januari 2017

KETUA
JURUSAN SISTEM INFORMASI

KEMENTERIAN RISET, TEKNOLOGI, DAN PENDIDIKAN TINGGI
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
FAKULTAS TEKNOLOGI INFORMASI
JURUSAN SISTEM INFORMASI

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

PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO/IEC 27002 : 2013 PADA IS-NET JURUSAN SISTEM INFOMASI ITS

TUGAS AKHIR

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

Oleh :

SALMAN AL FARISI

5209 100 058

Disetujui Tim Penguji : Tanggal Ujian : 6 Januari 2017
Periode Wisuda : 4 Maret 2017

Dr. Apol Pribadi S., S.T., M.T **(Pembimbing1)**

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

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

Eko Wahyu Tyas Diningrat, S.Kom, MBA **(Penguji 2)**

PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO/IEC 27002 : 2013 PADA IS-NET JURUSAN SISTEM INFOMASI ITS

Nama Mahasiswa : SALMAN AL FARISI
NRP : 5209100058
Jurusan : Sistem Informasi FTIf – ITS
Dosen Pembimbing 1 : Dr. Apol Pribadi S, S.T, M.T
Dosen Pembimbing 2 : Anisah Herdiyanti, S.Kom, M.Sc

ABSTRAK

IS-Net merupakan pusat pengelolaan sistem atau teknologi informasi yang digunakan untuk membantu mencapai tujuan akademik di jurusan Sistem Informasi (JSI) ITS dalam pengimplementasian Teknologi Informasi (TI). Pengimplementasian TI tersebut tidak serta merta berjalan dengan mulus namun sebaliknya pengimplementasiannya memiliki banyak hambatan, ancaman, serta risiko yang dapat merugikan organisasi baik dari segi finansial maupun non-finansial, bahkan pengimplementasiannya tidak berjalan sesuai dengan yang diharapkan terutama di bagian keamanan fisik dan lingkungan. Maka dari itu, diperlukan pengelolaan risiko-risiko yang ada dan yang akan terjadi sehingga tujuan organisasi dalam pengimplementasian TI dapat tercapai. Sebelumnya telah ada peneliti lain yang melakukan pengidentifikasian, penilaian risiko di IS-NET serta memberikan kontrol terhadap risiko yang telah diidentifikasi dengan menggunakan standard ISO 27001 dan 27002, namun hal tersebut tidak menjamin bahwa kontrol yang telah diberikan akan dilakukan oleh pihak IS-NET, sehingga diperlukan kegiatan audit untuk mengecek bahwa kontrol yang diberikan telah dilakukan atau tidak. Dalam melaksanakkan kegiatan audit perlu adanya buku panduan audit agar proses audit yang dilakukan lebih terstruktur dan tepat sasaran. Dari

hal tersebut, maka buku panduan audit dibutuhkan terutama untuk keamanan fisik dan lingkungan.

Hasil dari Tugas Akhir ini adalah sebuah panduan audit berbasis risiko pada IS-NET Jurusan Sistem informasi yang berisi dokumen audit plan dan audit program yang mengacu pada standard ISO/IEC 27002:2013 klausul keamanan fisik dan lingkungan

Kata Kunci**: **Teknologi Informasi, Audit TI, Audit Berbasis Risiko, Keamanan Fisik dan Lingkungan, ISO/IEC 27002:2013, Panduan Audit

DESIGNING INFORMATION TECHNOLOGY PHYSICAL AND ENVIRONMENTAL SECURITY RISK BASED AUDIT GUIDELINE BASED ON ISO/IEC 27002 :2013 IN IS-NET DEPARTEMENT INFORMATION SYSTEM ITS

Name	**:**	**SALMAN AL FARISI**
NRP	**:**	**5209100058**
Department	**:**	**Information Systems, FTif – ITS**
Supervisor 1	**:**	**Dr. Apol Pribadi S, S, S.T., M.T**
Supervisor 2	**:**	**Anisah Herdiyanti, S.Kom., M.Sc**

ABSTRACT

IS-Net is a central management or information technology systems that are used to help achieve the goals of academic major Information Systems (JSI) ITS for implementing Information Technology (IT). Implementation of IT wasn't done smoothly, but otherwise its implementation has many obstacles, threat and risk that can be detrimental to the organization, terms of both financial and non-financial, even that implementation doesn't be run as expected, especially in the physical security and the environment. Therefore, its necessary to manage of the risks and it will happen until organization goals can be achieved in the implementation of IT. There had been other researchers were conducting identification, risk assessment at IS-NET and provide control over the risks that have been identified using standard ISO 27001 and 27002, but it does not guarantee that the controls that have been given will be carried out by the IS-NET, so audit activities are needed to check the controls provided have been done or not. In the implementation of audit activities necessary to guide a book to the audit process conducted more structured and targeted. Cause of that, the audit guide books needed primarily for physical security and the environment.

The result of this final project is a guide to the risk based audit on IS-NET Department information system that contains the

document audit plan and audit program referring to the standard ISO / IEC 27002: 2013 clause physical and environmental security

Keywords : : Information Technology, IT Audit, Risk-Based Audit, Physical Security and Environment, ISO / IEC 27002: 2013, the Audit Guidance

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan pada Allah SWT yang telah memberikan rahmat dan ridhonya kepada penulis sehingga dapat menyelesaikan buku tugas akhir dengan judul **"PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO 27002 : 2013 PADA IS-NET JURUSAN SISTEM INFORMASI ITS"**

Sebagai salah syarat untuk memperoleh gelar Sarjana Komputer di Jurusan Sistem Informasi – Institut Teknologi Sepuluh Nopember Surabaya.
Pada kesempatan ini, penulis ingin menyampaikan terima kasih kepada semua pihak yang telah memberikan doa, dukungan, bimbingan, arahan, bantuan, dan semangat dalam menyelesaikan tugas akhir ini, yaitu kepada:

1. Bapak Dr. Ir.Aris Tjahyanto, M.Kom, selaku Ketua Jurusan Sistem Informasi ITS
2. Bapak Dr. Apol Pribadi Subriadi, S.T, M.T, selaku dosen pembimbing 1 yang telah meluangkan waktu dan pikiran untuk mendukung dan membimbing dalam penyelesaian tugas akhir penulis.
3. Ibu Anisah Herdiyanti, S.Kom., M.Sc selaku dosen pembimbing 2 yang telah memberikan pengarahan selama penulis menempuh masa perkuliahan dan penelitian tugas akhir.
4. Pak Hermono, selaku admin laboratoriun PPSI yang membantu penulis dalam hal administrasi penyelesaian tugas akhir dan mendukung penyelesaian tugas akhir ini.
5. Orang tua dan keluarga penulis yang telah mendoakan dan senantiasa mendukung serta selalu memberikan semangat dalam penyelesaian tugas akhir ini.
6. Terima kasih kepada Nur Aini yang selalu mendukung dan memberikan semangat serta menemani penulis untuk menyelesaikan tugas akhir ini.

7. Pihak-pihak lain yang telah mendukung dan membantu dalam kelancaran penyelesaian tugas akhir.

Penyusunan laporan ini masih jauh dari sempurna, untuk itu penulis menerima adanya kritik dan saran yang membangun untuk perbaikan di masa mendatang. Semoga buku tugas akhir ini dapat memberikan manfaat bagi para pembaca dan menjadi sebuah kontribusi bagi ilmu pengetahuan.

Surabaya, Januari 2017

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

halaman ini sengaja dikosongkan

BAB I
PENDAHULUAN

Pada bab ini akan dijelaskan latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat yang diperoleh, target luaran, dan sistematika penulisan yang ingin dicapai dalam pengerjaan Tugas Akhir.

1.1 Latar Belakang

Dewasa ini perkembangan teknologi informasi (TI) sangatlah pesat dan telah menjadi sesuatu yang penting bagi sebuah organisasi untuk mencapai tujuannya. Pemanfaatan Teknologi informasi tidak hanya sebagai alat pendukung saja. Namun, pemanfaatan teknologi informasi tersebut dapat dijadikan sebagai *Strategic Improvement* agar organisasi tersebut tetap bisa bersaing dengan kompetitor-kompetitor lain [**1**]. Seiring berjalannya waktu banyak Perguruan Tinggi yang mulai mengembangkan dan memanfaatkan TI untuk meningkatkan pelayanannya terhadap karyawan, dosen dan mahasiswa. Salah satu contoh manfaat TI bagi karyawan adalah dapat membantu dan memudahkan proses administrasi, sedangkan manfaat TI bagi Mahasiswa dan Dosen yaitu dapat membatu proses belajar mengajar. Dengan memanfaatkan TI, sebuah Perguruan Tinggi dapat mewujudkan tujuannya untuk menciptakan Sumber Daya Manusia (SDM) yang menguasai TI [**2**].

Pemanfaatan TI tidak selalu meberikan dampak yang positif. Namun, juga dapat memberikan dampak yang negatif apabila tidak didukung dengan keamanan fisik dan lingkungan TI yang baik. Keamanan Fisik dan Lingkungan TI yang dimaksud meliputi kondisi infrastruktur TI, tata letak, fasilitas yang tersedia, pengamanan akses fisik tersebut. Pengelolaan pengamanan fisik dan lingkungan TI yang baik akan mengurangi gangguan bisnis dari risiko-risikokerusakan perangkat TI, kehilangan data karena pencurian, kebakaran dan lain-lain [**3**].

Jurusan Sistem Informasi (JSI) merupakan salah satu jurusan di Institut Teknologi Sepuluh Nopember (ITS) yang menggunakan teknologi informasi dalam kegiatan sehari-hari. dengan adanya TI Segenap civitas di JSI sangat terbantu dalam melakukan kegiatan yang dilakukan. JSI memiliki pusat pengelolaan data dan informasi yang dinamakan IS-NET. Proses bisnis utama dari IS-Net ini adalah sebagai *server database* serta *gateway* akses wifi yang ada di seluruh JSI. Sebagai server di JSI, di dalam IS-NET terdapat server dari website JSI, CCTV, *database* SITV, *database finger print*, aplikasi keluhan, *database* nilai dan absensi, serta data sharing antara mahasiswa dan dosen JSI. Dari pengimplementasian TI tersebut juga mengharuskan JSI memiliki aset TI yang cukup banyak dan tidak menuntut kemungkinan aset TI tersebut juga memiliki banyak ancaman yang dapat menjadi risiko yang menyebabkan JSI mengalami kerugian sehingga diperlukan perlindungan keamanan. Dalam penerapan atau pengimplementasian TI di JSI itu sendiri masih kurang *aware* terhadap keamanan informasi.Buktinya seperti yang telah dipaparkan dalam penelitian sebelumnya bahwa di IS-NET memiliki banyak risiko sehingga oleh peneliti risiko-risiko tersebut di berikan kontrol sebagai upaya memitiigasi risiko yang ada.namunhal tersebut tidak menjamin bahwa kontrol yang telah diberikan akan dilakukan oleh pihak IS-NET.

Sebuah organisasi jika ingin mencapai tujuannya, maka organisasi tersebut harus memeriksa semua kontrol yang bertujuan mengurangi semua risiko yang mengancam pencapaian tujuan tersebut [**4**].maka dari itu diperlukan adanya pemeriksaan untuk memastikan bahwa semua kontrol yang diberikan telah dilakukan dengan baik sebagai tindakan untuk mengurangi risiko. Pemeriksaan tersebut dilakukan dengan cara mengadakan kegiatan Auditdengan berbasiskan risiko. Untuk melaksanakan kegiatan audit dengan baik diperlukan membuat beberapa perencanaan dan persiapan yang baik sebelum melaksanakan kegiatan audit tersebut.Maka dari itu perlu adanya perangkat atau panduan yang bisa digunakan untuk membantu dan memudahkan proses audit secara

terstruktur dan tidak sembarangan.Sementara ruang lingkup yang akan diteliti pada penelitian ini mengacu pada penelitian sebelumnya yang diteliti oleh Krisna H Dewantara (2016) yang menjelaskan bahwa kontrol yang diberikan pada risiko-risiko yang merupakan risiko yang *high* dan *very high*untuk memitigasi risiko paling banyak memakai kontrol yang ada pada ISO/IEC 27002 klausul keamanan fisik dan lingkungan [**5**].

Berdasarkan hal tersebut, maka tugas akhir ini bertujuan untuk merumuskan Panduan Audit Keamanan Fisik dan Lingkungan Teknologi informasi berbasis risiko berdasarkan ISO/IEC 27002:2013pada IS-NET Jurusan Sistem Informasi ITS. Panduan audit ini diharapkan dapat membantu jalannya proses audit oleh auditor. Hasil dari tugas akhir ini terdiri dari penjelasan mengenai tujuan, ruang lingkup, informasi auditee dan auditor, acuan dan penanggung jawab audit, prosedur audit, audit checklist, dan formulir lain yang mendukung proses audit..

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka berikut perumusan masalah yang akan diselesaikan pada tugas akhir ini:

1. Seperti apa usulan *Audit Plan* yang dibuat?
2. Seperti apa usulan *audit program* yang dibuat?

1.3 Batasan Masalah

Tugas akhir ini memiliki batasan pengendalian pengerjaan untuk fokus pada permasalahan yang dibahas. Maka berikut batasan masalah dalam tugas akhir ini:

1. Ruang lingkup yang akan diteliti berfokus pada ruangan IS-NET di Jurusan Sistem informasi.
2. Standart atau framework yang digunakan untuk membuat panduan audit SI/TI adalah ISO/IEC 27002:2013 klausul keamanan fisik dan lingkungan

3. Dokumen panduan audit SI/TI difokuskan pada 2 (dua) bagian yaitu Dokumen *Audit Plan* dan *Audit Program*.

1.4 Tujuan Penulisan

Tujuan dari pengerjaan tugas akhir ini adalah untuk menghasilkan dokumen panduan audit yang nantinya akan membantu auditor yang terdiri dari *Audit Plan* dan *audit Program*

1.5 Manfaat Penulisan

Manfaat yang diberikan dari pengerjaan tugas akhir ini adalah sebagai berikut:

Bagi akademis

1. Memberikan sumbangsih pengetahuan mengenai pembuatan panduan Audit terkait keamanan fisik dan lingkungan berdasarkan ISO/IEC 27002:2013
2. Menambah referensi pada penelitian selanjutnya yang berkaian dengan pembuatan panduan audit

Bagi perusahaan

1. Memberikan usulan dokumen Panduan Audit Keamanan fisik dan lingkungan di IS-NET yang dapat digunakan perusahaan di masa yang akan datang

1.6 Relevansi Tugas Akhir

Penelitian tugas akhir ini memiliki relevansi dengan mata kuliah yang diajarkan di Jurusan Sistem Informasi ITS yaitu mata kuliah Manajemen Layanan Teknologi Informasi, Tata Kelola Teknologi Informasi, Manajemen Risiko Teknologi Informasi, dan Audit.

BAB II
TINJAUAN PUSTAKA

Pada bab ini akan menjelaskan mengenai penelitian sebelumnya dan dasar teori pendukung yang akan dijadikan acuan atau landasan dalam pengerjaan tugas akhir ini.

2.1 Studi Sebelumnya

Dalam penelitian ini, digunakan beberapa penelitian terdahulu sebagai pedoman dan referensi mengenai pembuatan audit program dan panduan audit. Tabel 1-4 menyajikan penelitian-penelitian sebelumnya yang berisi tentang pembuatan panduan audit teknologi informasi dimana penelitian tersebut dijadikan referensi oleh penulis dalam pengerjaan tugas akhir.

Tabel 2.1 Penelitian Sebelumnya 1

Nama Peneliti	**Fandy Natahiwidha (2010)**
Judul Penelitian	Pembuatan Audit program Jaringan CSNET Berdasarkan Cobit 4.1 dan ISO 27002 Pada Jurusan Sistem Informasi Institut Teknologi Sepuluh Nopember [**6**].
Hasil Penelitian	Penelitian ini menghasilkan audit program yang dapat digunakan untuk mengaudit keamanan NOC CSNet sehingga pihak JSi dapat mengetahui ketidaksesuaian dari perlindungan keamanan yang sudah ada saat ini. Penelitian ini mengacu pada audit konvensiaonal atau finansial audit
Relevansi	Pendekatan yang dipakai dalam pembuatan panduan/audit program ini tidak sama. Penelitian ini menggunakan pendekatan audit konvensional atau biasa disebut dengan finansial audit sedangkan penulis menggunakan Audit berbasiskan risiko dimana berdasarkan risiko yang

	telah diidentifikasi dan diprioritaskan kemudian dicari risiko yang paling rawan yang mengancam organisasi serta kontrol yang paling banyak dipakai pada risiko tersebut dijadikan ruang lingkup penelitian

Tabel 2.2 Penelitian Sebelumnya 2

Nama Peneliti	**Yudhis Cahyo Eko (2013)**
Judul Penelitian	Pembuatan Panduan Audit Teknologi Informasi pada Proses Pengelolaan Lingkungan Fisik berbasis COBIT 5 di KPPN Surabaya II [**3**].
Hasil Penelitian	Penelitian ini berisi pembuatan panduan audit yang berbasis pada COBIT 5. Panduan Audit yang dibuat meliputi ikhtisar dokumen panduan audit, kertas kerja pemeriksaan utama, *audit checklist*, prosedur audit, dan kertas kerja konsep temuan.
Relevansi	Fokus penelitian saat ini adalah membuat panduan audit, sama dengan apa yang dilakukan pada penelitian 2 ini sehingga akan memudahkan penulis untuk mengetahui apa saja yang harus disusun dalam panduan audit.

Tabel 2.3 Penelitian Sebelumnya 3

Nama Peneliti	**Stephen Christian (2015)**
Judul Penelitian	Pembuatan Panduan Audit Keamanan Fisik dan Lingkungan Teknologi Informasi Berbasis Risiko berdasarkan ISO 27002 : 2013 pada Direktorat Sistem Informasi Universitas Airlangga [**7**]
Hasil Penelitian	Penelitian ini berisi pembuatan panduan audit yang berupa audit plan dan audit

	program dengan acuan ISO/IEC 27002 klausul keamanan fisik dan lingkungan TI paada direktorat sistem informasi Universitas Airlangga. Hal-hal yang akan diaudit antara lain Direktur Sistem Informasi, administrator, database, dan peraturan lain yang terkait.
Relevansi	Penulis menggunakan penelitian ini untuk membantu dalam mengerjakan Tugas Akhir dalam hal pemetaan dalam ISO/IEC 27002. Dengan menggunakan standar yang sama dan lingkungan yang hampir sama pula dan diharapkan pemetaan yang dilakukan penulis lebih tepat.

Tabel 2.4 Penelitian Sebelumnya 4

Nama Peneliti	**Krisna Harinda Dewantara (2016)**
Judul Penelitian	Identifikasi, Penilaian, dan Mitigasi Risiko Keamanan Informasi berdasarkan Standar ISO 27001:2005 dan ISO 27002: 2013 menggunakan Metode FMEA(Studi Kasus : IS-Net) [**5**].
Hasil Penelitian	Penelitian ini berisi tentang proses mengidentifikasi, penilaian, serta memitigasi risiko menggunakan standar ISO 27001 dan 27002 serta Metode FMEA dalam menilai dan memprioritaskan risiko di IS-NET hasilnya adalah *risk register* yang telah diberikan kontrol untuk memitigasi risiko-risko yang ada di IS-NET
Relevansi	• Organisasi tempat penelitian dilakukan, menguatkan penulis untuk melakukan Tugas Akhir dengan topik audit sehingga dapat dijadikan referensi yang sangat bagus bagi

	penulis. • Berdasarkan risiko yang telah diberikan kontrol untuk memitigasinya penulis melatarbelakangi untuk membuat panduan audit serta kontrol yang paling banyak digunakan pada risiko yang tergolong high dan very high sebagai ruang lingkup penelitian penulis

2.2 Dasar Teori

Pada bagian ini, akan dijelaskan mengenai teori-teori yang digunakan untuk mendukung pengerjaan tugas akhir. Teori tersebut yaitu mengenai: Audit, Audit SI/TI, audit berbasis risiko, panduan audit, risiko, manajemen risiko TI, keamanan informasi, aset informasi, sistem manajemen keamanan informasi, ISO 27002: klausul keamanan fisik dan lingkungan, FMEA, proses manajemen proyek, dan metode *step wise*.

2.2.1 Audit

Auditing adalah suatu pemeriksaan yang dilakukan secara kritis dan sistematis, oleh pihak independen, terhadap laporan keuangan yang telah disusun oleh manajemen beserta catatan-catatan pembukuan dan bukti-bukti pendukungnya, dengan tujuan untuk dapat memberikan pendapat mengenai kewajaran laporan keuangan tersebut [**8**].

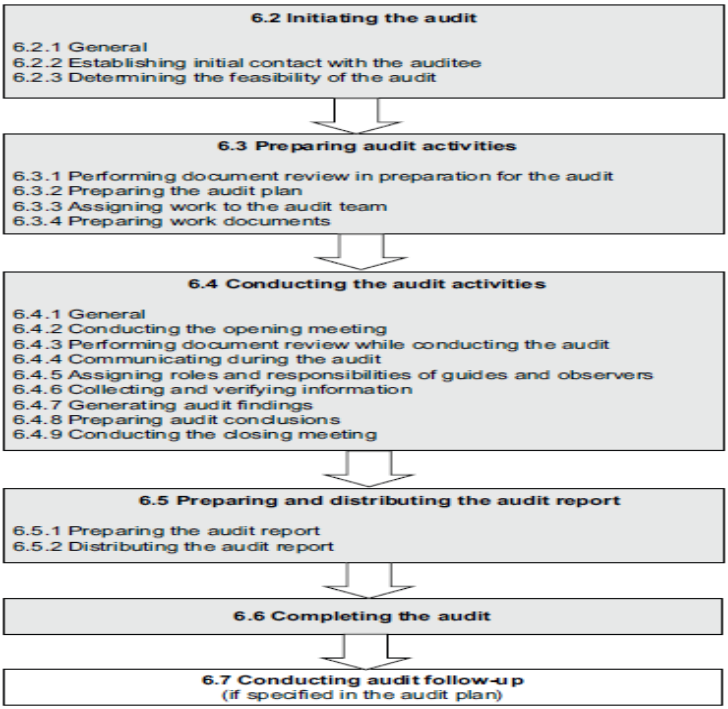
Menurut Alvin A. Arens dan James K. Loebbecke [**9**] audit adalah kegiatan mengumpulkan bukti dan mengevaluasi dari bukti-bukti mengenai informasi untuk menentukan dan melaporkan tingkat kesesuaian antara informasi dengan kriteria yang telah ditetapkan.

Sedangkan Audit menurut William F Meisser, Jr adalah proses yang sistematik dengan tujuan mengevaluasi bukti mengenai tindakna dan kejadian ekonomi untuk memastikan tingkat kesesuaian antara penugasan dan kriteria yang telah

ditetapkan, hasil dari penugasan tersebut dikomunikasikan kepada pihak pengguna yang berkepentingan [**10**].

dari beberapa pengertian diatas audit dapat didefinisikan suatu kegiatan yang dilakukan guna untuk memeriksa sebuah kepatuhan pengelolaan proses (kesesuaian) dan bukti yang dapat terukur dengan tujuan organisasi yang didasarkan pada sebuah standard atau acuan yang biasanya digunakan adalah *best practice*.

Secara garis besar proses Audit dalam ISO 19011:2011 [**11**]sebagai berikut:



Gambar 2.1 Proses Audit Pada ISO 19011:2011

Berikut ini adalah penjelasan dari gambar diatas :

1. *Initiating the Audit*

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

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

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

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

2. *Preparing audit activities*

Hal yang perlu diperhatikan dalam tahap persiapan aktivitas audit adalah

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

2.2 Menyiapkan dokumen *audit plan*

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

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

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

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

2.3 Pemberian tugas pada tim audit

Ketua tim audit berhak memberikan tanggung jawab kepada setiap anggota tim audit untuk mengaudit proses, aktivitas fungsi, atau lokasi tertentu. Perubahan terhadap tugas yang diberikan dapat dilakukan saat proses audit berlangsung untuk memastikan tujuan audit terpenuhi.

2.4 Menyiapkan dokumen kerja

anggota tim audit harus mengumpulkan dan meninjau ulang informasi yang berkaitan dengan tugas audit masing-masing anggota dan menyiapkan dokumen kerja. Dokumen kerja yang dimaksud antara lain adalah:

a. *Checklist*

b. rencana *audit sampling*
c. formulir untuk pencatatan bukti audit, temuan audit, dan catatan rapat.

3. *Conducting the audit activities*

Aktivitas audit umumnya dilaksanakan seperti yang tertera pada Gambar yaitu:

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

4. *Preparing and distributing the audit report*

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

5. *Completing the audit*

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

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

6. *Conducting audit follow-up*

Kesimpulan dari audit yang dilakukan mungkin saja memerlukan perbaikan, baik itu aksi *corrective, preventive,* atau *improvement*. Kegiatan tersebut biasanya dilakukan oleh *auditee* dalam kurun waktu tertentu yang sudah disetujui.

Auditee juga harus menghubungi dan mengkomunikasikan tim audit mengenai status kegiatan perbaikan yang dilakukan.
Dari seluruh proses yang ada (proses 1-6) dalam pengerjaan Tugas Akhir ini hanya akan digunakan proses 1 dan 2 karena penulis tidak sampai pada tahap melakukan proses audit.

2.2.2 Audit SI/TI

Menurut Ron Weber Audit TI merupakan proses pengumpulan dan evaluasi bukti-bukti untuk menentukan apakah system computer yang digunakan telah dapat melintungi aset milik organisasi, mampu menjaga integritas data, dapat membantu pencapaian tujuan organisasi secara efektif, serta menggunakan sumber daya yang dimiliki secara efisien [**12**].

Menurut Gondodiyoto audit sistem informasi merupakan suatu pengevaluasian untuk mengetahui bagaimana tingkat kesesuaian antara aplikasi sistem informasi dengan prosesdur yang telah ditetapkan dan mengetahui apakah sustu sistem informasi tersebut telah didesain dan diimplementasikan secara efektif, efisien, dan ekonomis memiliki mekanisme pengamanan asset yang memedai, serta menjamin integritas data yang memadai [**13**].

Sedangkan Audit Sistem informasi menurut Sarno dalam bukunya "Audit Sistem/teknologi informasi" adalah aktivitas audit yang dilakukan untuk memastikan pengelolaan sistem informasi sehingga terarah dalam kerangka perbaikan berkelanjutan dan penyesuaian terhadap kepatuhan apakah sistem berjalan sesuai dengan standard [**14**].

Dalam ISA ruang lingkup Audit TI tidak jauh kiprahnya dari siklus aktifitas IT korporasi (lihat gambar) yang secara sederhana terdiri dari 4 area [**15**]:

1. Pengembangan Perangkat lunak dan Sistem Aplikasi (*System Development*)
2. Dukungan Jaringan IT (*IT Network Support*)
3. Pusat Pengelolaan Data (*Data Center*) dan Administrator Sistem (*System Administrator*)

4. Pengoperasian Sistem oleh User (*System User*)

2.2.3 Audit Berbasis Risiko

Risk Based Auditing adalah audit yang difokuskan dan diprioritaskan pada risiko bisnis dan prosesnya serta pengendalian terhadap risiko yang dapat terjadi [**16**].

Dengan demikian audit berbasis risiko berfungsi mulai dari saat penetapan tujuan perusahaan sampai kepada upaya untuk mencapai tujuan tersebut dengan memberikan fokus lebih kepada risiko (termasuk kontrol) yang telah diidentifikasi oleh manajemen, khususnya risiko yang dapat menggagalkan pencapaian tujuan perusahaan.

Menurut ISA proses Audit berbasis Risiko memiliki tiga langkah kunci yaitu [**17**]:

1. Menilai Risiko (*Risk Assessment*)
   Pada tahap ini auditor bertujuan untuk mengidentifikasi dan menilai salah saji yang material, karena kecurangan atau kesalahan, pada tingkat lapporan keuangan dan asersi, melalui pemahaman terhadap entitas dan lingkunganya, termasuk pengendalian intern entitas, yang memberikan dasar untuk merancang dan mengimplementasi tanggapan terhadap risiko yang dinilai.
2. Menanggapi Risiko (*Risk Response*)
   Selanjutnya pada tahap ini auditor bertujuan untuk memperoleh bukti yang cukup dan tepat tentang risiko yang dinilai, dengan merancang dan mengimplementasi tanggapan yang tepat terhadap risiko tersebut.
3. Pelaporan (*Reporting*)
   Untuk tahap yang terakhir auditor bertujuan untuk merumuskan opini mengenai laporan keuangan berdasarkan evaluasi atas kesimpulan yang ditarik atas bukti audit yang diperoleh, dan memberikan opini dengan jelas, melalui laporan tertulis, yang juga

menjelaskan dasar (untuk memberikan) pendapat tersebut.

2.2.4 Jenis Audit

Menurut Abdul Halim, dilihat dari sisi luas pemeriksaan dan untuk siapa audit dilaksanakan, audit dapat dikelompokkan menjadi tiga jenis golongan, berikut diantaranya [16]:

1. Audit Eksternal – merupakan suatu kontrol sosial yang memberikan jasa untuk memenuhi kebutuhan informasi untuk pihak luar perusahaan yang diaudit. Pelaksana audit eksternal adalah auditor dari pihak luar perusahaan yang independen dan telah diakui oleh pihak berwenang untuk melaksanakan tugas tersebut. Auditor eksternal pada umumnya dibayar oleh manajemen perusahaan yang diaudit.
2. Audit Internal – merupakan suatu kontrol organisasi yang mengukur dan mengevaluasi efektivitas organisasi. Informasi yang dihasilkan, ditujukan untuk manajemen organisasi itu sendiri. Pelaksana audit internal adalah auditor internal dan merupakan karyawan organisasi tersebut. Berfungsi membantu meningkatkan efisiensi dan efektivitas kegiatan perusahaan.
3. Audit Sektor Publik – suatu kontrol atas organisasi pemerintah yang memberikan jasanya pada masyarakat, seperti pemerintah pusat maupun pemerintah daerah. Audit dapat mencakup audit laporan keuangan, audit kepatuhan, maupun audit operasional. Pelaksana audit sektor publik disebut dengan auditor pemerintah dan dibayar oleh pemerintah.

Pada penelitian ini, pembuatan panduan audit ditujukan untuk audit internal di mana proses pelaksanaan pemeriksaan atau audit dilakukan oleh auditor internal organisasi dikarenakan audit yang akan dilakukan bertujuan untuk mengevaluasi

pengelolaan proses bisnis di organisasi sehingga dapat mengurangi risiko yang ada.

2.2.5 Panduan Audit

Buku panduan adalah buku yang menyajikan informasi dan memandu atau memberikan tuntunan kepada pembaca untuk melakukan apa yang disampaikan dalam buku tersebut [**18**]. Sebuah buku panduan dikatakan berhasil apabila panduan yang disampaikan di dalam buku tersebut dapat dipahami dan diterapkan dengan baik oleh pembacanya.

Buku Panduan Audit adalah buku yang menyajikan informasi untuk memandu serta memberikan tuntunan dalam melakukan proses audit oleh auditor. Tujuan buku audit dibuat adalah untuk memudahkan auditor dan auditee dalam melakukan kegiatan audit dan proses-prosesnya dapat dimengerti serta pelaksanan audit dapat berjalan dengan lancar dan terstruktur.

Panduan Audit secara garis besar dibagi menjadi beberapa bagian yaitu:

a. Dokumen *Audit Charter*
   Audit Charter adalah sebuah dokumen resmi yang mendefinisikan tujuan, wewenang, dan tanggung jawab aktivitas audit internal [**19**]. Posisi proses audit internal dalam organisasi ditetapkan dalam *Audit Charter*. Hal ini termasuk sifat hubungan pelaporan fungsional kepala Audit eksekutif dengan dewan; kewenangan akses terhadap catatan, personel, dan sifat fisik yang relevan dengan kinerja keterlibatan; dan mendefinisikan ruang lingkup kegiatan audit internal. Persetujuan akhir dari *Audit Charter* adalah dengan jajaran eksekutif.

b. Dokumen *Audit Plan*
   Audit Plan adalah pedoman khusus yang harus diikuti ketika melakukan audit. *Audit Plan* menggambarkan proses-proses yang harus dilakukan oleh auditor untuk dapat mencapai tujuan audit [**11**]. Hal ini akan membantu auditor memperoleh bukti yang cukup dan

tepat, membantu menjaga biaya audit pada tingkat yang wajar, dan membantu menghindari kesalahpahaman dengan klien.

Audit Plan setidaknya mencakup hal-hal berikut:

1. Apa tujuan audit dilaksanakan?
2. Kapan audit akan dilaksanakan?
3. Dimana audit akan dilaksanakan?
4. Siapa saja auditornya?

Dalam dokumen perencanaan audit berisikan sebagai berikut:

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

c. Dokumen *Audit Program*

Menurut TYBCom Accountancy Auditing sebuah audit program merupakan daftar-daftar pemeriksaan dan langkah verifikasi yang ditetapkan sedemikian rupa sehingga antara langkah satu dengan langkah yang lain menunjukkan suatu hubungan yang jelas dan akan menjadi dasar dalam membuat suatu pelaporan. Audit program dapat pula berisi sebuah prosedur yang ditunjukkan dengan sebuah instruksi yangdapat digunakan untuk mencapai tujuan audit

Dalam membuat audit program ada beberapa hal yang perlu diperhatikan seperti:

1. Audit program harus mencakup scope dan batasan audit
2. Menentukan bukti yang beralasan (berdasarkan fakta) dan melakukan identifikasi bukti terbaik
3. Hanya menerapkan prosedur yang telah terverifikasi

4. Selalu mempertimbangkan semua kemungkinan kesalahan yang akan terjadi
5. Mengkoordinasikan prosesdur sesuai dengan aktifitas terkait

Top Management harus memastikan bahwa tujuan program audit ditetapkan dan menetapkan satu atau lebih kompeten orang untuk mengelola program audit. Ruang lingkup program audit harus didasarkan pada ukuran dan sifat organisasi yang diaudit, serta pada sifat, fungsi, kompleksitas dan tingkat kematangan sistem manajemen yang diaudit [**11**].

Menurut ISO 19011 [**11**], program audit harus mencakup informasi dan sumber daya yang diperlukan untuk mengatur dan melakukan audit secara efektif dan efisien dalam kerangka waktu tertentu dan juga dapat mencakup sebagai berikut:

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

Dalam pembuatan panduan audit terdapat beberapa dokumen kerja yang dapat dibuat yaitu dokumen prosedur audit, daftar cek berdasarkan prosedur dan dokumen tambahan seperti audit report yang dapat dibuat sesuai dengan kebutuhan seperti pencatatan daftar temuan, hasil evaluasi, data penanggung jawab, data auditor, solusi, catatan dari manajemen perusahaan, dan laporan-laporan lainnya.

Berikut beberapa penjelasan singkat mengenai audit program yang akan dibuat pada penulisan ini mengacu IS/ISO 19011:2011:

1. Prosedur Audit

Dokumen prosedur atau skenario langkah-langkah untuk setiap kontrol yang telah dianalisa. Pada prosedur audit ini di dalamnya akan berisi langkah-langkah sesuai dengan control yang dilengkapi dengan *flow activity.*

2. Daftar Cek

Daftar cek ini dibuat untuk mengetahui apakah aktivitas yang ada pada setiap prosedur sudah atau belum berjalan. Dimana dalam daftar cek ini akan dilengkapi dengan tempat penulisan sebuah bukti (*evidence*) yang akan membantu auditor untuk membuat temuan dan dicatatkan pada *audit report.*

3. Audit Report

Dibuat sesuai dengan kebutuhan seperti pencatatan daftar temuan, hasil evaluasi, data penanggung jawab, data auditor, solusi, catatan dari manajemen perusahaan, dan laporan-laporan lainnya

4. Panduan Penggunaan Program Audit

Panduan ini dibuat untuk memudahkan tim audit internal untuk melakukan audit dan mengoperasikan perangkat yang telah dibuat. Panduan penggunaan audit program ini nantinya akan berisi langkah-langkah dan tata-cara penggunaan audit program yang telah dibuat pada tahapan sebelumnya.

Dalam pengerjaan Tugas Akhir ini, dokumen panduan audit hanya berfokus pada *Audit Plan* dan *Audit Program* saja. *Audit program* yang dibuat akan mengacu pada penelitian milik Krisna H Dewantara [**5**],

dimana akan terjadi beberapa penyesuaian. *Audit program* yang disusun penulis berisi:

a. Tujuan dan ruang lingkup audit,
b. *Best practice* dan kendali tujuan,
c. Prosedur dan daftar cek audit,
d. *Audit Report*,
e. Panduan penggunaan *audit program*

2.2.6 Risiko

David Mc Namee dan Georger selim [**20**] memberikan definisi tentang risiko sebagai suatu konsep yang digunakan untuk mengekspresikan ketidakpastian tentang kejadian yang dampaknya dapat memiliki efek atas pencapaian tujuan organisasi.

Risiko dapat didefinisikan sebagai perubahan atau perbedaan hasil yang tidak diharapkan [**21**]. Risiko begitu komplek dalam berbagai bidang yang berbeda, sehingga terdapat berbagai pengertian pula.

David Griffiths dalam bukunya [**4**] mendefinisikan risiko sebagai suatu keadaan yang dapat menghambat organisasi dalam mencapai tujuan yang telah ditetapkan (*a risk a set of circumstances that hinder the achievement of objective*). Oleh karena itu, semua risiko yang ada dan akan terjadi harus dikelola dengan baik [**22**]

2.2.7 Risiko pada IS-Net

IS-Net Merupakan pusat pengelolaan sistem dan teknologi informasi yang digunakan untuk membantu mencapai tujuan akademik di jurusan Sistem Informasi (JSI)Institut Teknologi Sepuluh Nopember. Sebagai pusat pengelolaan sistem dan teknologi informasi IS-Net diharuskan memiliki aset yang cukup untuk membantu tercapainya tujuan di JSI. Sehingga, tidak menutup kemungkinan aset-aset tersebut memiliki ancaman dan risiko yang dapat menyebabkan tujuan JSI tidak tercapai. Berikut ini adalah Tabel 2.5 yang menjelaskan daftar risiko menurut Krisna H Dewantara dalam penelitiannya yang telah diprioritaskan serta diberikan kontrol untuk memitigasi risiko [**5**]:

Tabel 2.5 Daftar risiko Penelitian sebelumnya

ID Risiko	Risiko	Kategori	Penyebab	Dampak	RPN	Level	Opsi Mitigasi	Bentuk Mitigasi	Kontrol (ISO 27001/27002)
H03	Server Down	Hardware	Adanya praktik ilegal dari seseorang yang tidak bertanggung jawab	Terhambatnya proes bisnis ISNet	392	VERY HIGH	Treat	Melakukan konfigurasi pembatasan akses pada server	Pengguna hanya diperbolehkan untuk mengakses ke layanan yang telah diizinkan (11.4.1)

ID Risiko	Risiko	Kategori	Penyebab	Dampak	RPN	Level	Opsi Mitigasi	Bentuk Mitigasi	Kontrol (ISO 27001/27002)
			Terdapat kerentanan terhadap sistem keamanan server	Penurunan integritas ISNet			Treat	Melakukan konfigurasi pembatasan akses pada server	Integritas dari informasi tersedia untuk umum harus dilindungi untuk mencegah modifikasi yang tidak diizinkan (10.9.3)
			Banyak pengguna yang mengakses server dalam satu waktu	Penurunan tingkat kepercayaan pengguna ISNet Kerugian finansial & non-finansial			Treat	Melakukan konfigurasi pembatasan akses pada server	*Network* harus dikelola dan dikontrol untuk emlindunginya dari ancaman dan untuk menjaga keamanan sistem dan aplikasi yang menggunakan *network* tersebut termasuk informasi

ID Risiko	Risiko	Kategori	Penyebab	Dampak	RPN	Level	Opsi Mitigasi	Bentuk Mitigasi	Kontrol (ISO 27001/27002)
									didalamnya (10.6.1)
H15	Kerusakan kabel UTP	Hardware	Kerentanan alam dan lokasi	Terhambatnya proes bisnis ISNet	180	High	Take	Membuat *Disaster Recovery Plan*	Mendesain dan mengaplikasikan perlindungan fisik terhadap kerusakan yang disebabkan kebakaran, bajir, gempa bumi, ledakan, kerusuhan, dan bentuk lainnya yang berasal dari alam maupun manusia (9.1.4)

ID Risiko	Risiko	Kategori	Penyebab	Dampak	RPN	Level	Opsi Mitigasi	Bentuk Mitigasi	Kontrol (ISO 27001/27002)
			Jadwal pemadam mati listrik	●Terputusnya koneksi pada jaringan			Treat	Mempunyai genset cadangan untuk menyuplai listrik	Setiap aset harus dilindungi dari gangguan listrik dan gangguan lainnya yang disebabkan oleh kegagalan pada utilitas pendukung (9.2.2)
			Hewan yang mengigit kabel listrik				Treat	Meletakkan kabel pada tempat yang tidak dapat dijangkau hewan	Setiap aset harus dilindungi dari gangguan listrik dan gangguan lainnya yang disebabkan oleh kegagalan pada utilitas pendukung (9.2.2)

ID Risiko	Risiko	Kategori	Penyebab	Dampak	RPN	Level	Opsi Mitigasi	Bentuk Mitigasi	Kontrol (ISO 27001/27002)
			Beban listrik yang terlalu besar				Treat	Mengurangi penggunaan perangkat yang memiliki daya listrik yang besar yang tidak terlalu bermanfaat	Setiap aset harus dilindungi dari gangguan listrik dan gangguan lainnya yang disebabkan oleh kegagalan pada utilitas pendukung (9.2.2)
			Hubungan arus pendek				Treat	Mengurangi penumpukan steker/colokan listrik Melakukan peemeriksaan rutin terhadap kabel listrik	Setiap aset harus dilindungi dari gangguan listrik dan gangguan lainnya yang disebabkan oleh kegagalan pada utilitas pendukung (9.2.2)

ID Risiko	Risiko	Kategori	Penyebab	Dampak	RPN	Level	Opsi Mitigasi	Bentuk Mitigasi	Kontrol (ISO 27001/27002)
H16	Kabel UTP tidak dapat mentransfer data	Hardware	Kabel sering dicabut pasang	Terhambatnya proses bisnis ISNet	180	HIGH	Treat	Memberikan pengamanan, semacam rantai atau kunci.	Barang, informasi atau perangkat lunak tidak boleh diambil/dicabut dari tempatnya tanpa ada izin sebelumnya (9.2.7)
			Kabel digigit hewan	Terputusnnya koneksi internet yang ada di ISNet			Treat	Meletakan kabel pada lokasi yang aman dan terlindungi dari gangguan	Kabel tenaga dan telekomunikasi yang membawa data atau informasi pendukung harus terlindungi dari intersepsi atau kerusakan (9.2.3)
				Kerugian dari sisi finansial dan non-finansial					

ID Risiko	Risiko	Kategori	Penyebab	Dampak	RPN	Level	Opsi Mitigasi	Bentuk Mitigasi	Kontrol (ISO 27001/27002)
			Kelalaian pengguna	Terhambatnya proses bisnis ISNet			Treat	Memberikan sanksi kepada pengguna yang tidak bisa menjaga aset yang ia pakai	Pengguna harus memastikan bahwa aset tanpa pengawasan harus memiliki kebutuhan perlindungan atau sistem keamanan yang tepat (11.3.2)
P01	Tidak memiliki data backup	People	Tidak menggunakan konfigurasi RAID		100	MEDIUM	Treat	Memperbaharui prosedur dalam memback-up data yaitu dengan melakukan menggunakan konfigurasi RAID	Back-up informasi dan perangkat lunak harus ada dan sesuai dengan kebijakan back-up yang ada (10.5.1)

ID Risiko	Risiko	Kategori	Penyebab	Dampak	RPN	Level	Opsi Mitigasi	Bentuk Mitigasi	Kontrol (ISO 27001/27002)
			Ketidaksengajaan dan kelalaian dari admin dan laboran	Akan menjadi kerugian finansial apablia data utama hilang, apabila tidak membackup data tersebut sebelumnya			Treat	Memberikan pelatihan dan evaluasi kepada setiap laboran dan admin	Pihak manajemen harus mempunyai karyawan, kontraktor, dan pihak ketiga yang mematuhi kebijakan dan prosedur keamanan yang telah diterapkan pihak organisasi (8.2.1)
			Tidak adanya peringatan khusus dalam penjadwalan backup data				Treat	Membuat prosedur dan penjadwalan yang jelas untuk melakukan back-up data	Back-up informasi dan perangkat lunak harus ada dan sesuai dengan kebijakan back-up yang ada (10.5.1)

ID Risiko	Risiko	Kategori	Penyebab	Dampak	RPN	Level	Opsi Mitigasi	Bentuk Mitigasi	Kontrol (ISO 27001/27002)
			Proses back up data masih secara manual				Treat	Memperharui prosedur dalam memback-up data dengan melakukan otomasi konfigurasi backup data	Back-up informasi dan perangkat lunak harus ada dan sesuai dengan kebijakan back-up yang ada (10.5.1)
H01	Kehilangan Server	Hardware	Lokasi server yang mudah dijangkau	Terhambatnya proses bisnis ISNet	54	LOW	Treat	Mendesain lokasi server yang tidak mudah dijangkau dengan memindahkan lokasi server ke tempat yang lebih aman dari jangkauan orang lain.	Merancang dan menerapkan keamanan fisik untuk kantor, ruangan, dan lokasi falisitas dari ancaman luar (9.1.3)

ID Risiko	Risiko	Kategori	Penyebab	Dampak	RPN	Level	Opsi Mitigasi	Bentuk Mitigasi	Kontrol (ISO 27001/27002)
			Tidak ada pengamanan khusus berlapis pada server				Treat	Menerapkan sistem pengamanan fisik khusus untuk server ISNet menggunakan cage dan gembok pada ruangan.	Segala peralatan harus diletakkan atau dilindungi untuk mengurangi risiko dari ancaman lingkungan, bahaya, akses yang tidak legal (9.2.1)

ID Risiko	Risiko	Kategori	Penyebab	Dampak	RPN	Level	Opsi Mitigasi	Bentuk Mitigasi	Kontrol (ISO 27001/27002)
H04	Kerusakan Server	Hardware	Kerentanan alam dan lokasi	Terhambatnya proes bisnis	18	Very Low	Take	Membuat *Disaster Recovery Plan*	Mendesain dan mengaplikasikan perlindungan fisik terhadap kerusakan yang disebabkan kebakaran, bajir, gempa bumi, ledakan, kerusuhan, dan bentuk lainnya yang berasal dari alam maupun manusia (9.1.4)
			Aliran udara di server yang kurang baik	Penurunan integritas LPSI			Treat	Mengubah aliran udara pada Server menjadi lebih baik	Segala peralatan harus diletakkan atau dilindungi untuk mengurangi risiko dari ancaman lingkungan,

ID Risiko	Risiko	Kategori	Penyebab	Dampak	RPN	Level	Opsi Mitigasi	Bentuk Mitigasi	Kontrol (ISO 27001/27002)
									bahaya, akses yang tidak legal (9.2.1)
			Suhu ruangan yang terlalu panas	Penurunan tingkat kepercayaan pengguna LPSI			Treat	Melakukan *maintenance* secara berkala pada *AC*	Segala peralatan harus diletakkan atau dilindungi untuk mengurangi risiko dari ancaman lingkungan, bahaya, akses yang tidak legal (9.2.1)

ID Risiko	Risiko	Kategori	Penyebab	Dampak	RPN	Level	Opsi Mitigasi	Bentuk Mitigasi	Kontrol (ISO 27001/27002)
			Kualitas server yang kurang baik	Kerugian finansial & non-finansial			Treat	Melakukan *maintenance* secara berkala pada Server	Peralatan harus dipelihara dengan benar untuk memeastikan availability dan integrity-nya (9.2.4)
			Umur server yang sudah tua dan usang				Treat	Melakukan pembelian untuk melakukan penggantian terhadap komponen Server	Peralatan harus dipelihara dengan benar untuk memeastikan availability dan integrity-nya (9.2.4)

ID Risiko	Risiko	Kategori	Penyebab	Dampak	RPN	Level	Opsi Mitigasi	Bentuk Mitigasi	Kontrol (ISO 27001/27002)
			Terlalu banyak debu				Treat	Melakukan pembersihan pada PC secara berkala	Segala peralatan harus diletakkan atau dilindungi untuk mengurangi risiko dari ancaman lingkungan, bahaya, akses yang tidak legal (9.2.1)
			Jadwal pemadam mati listrik				Treat	Mempunyai genset cadangan untuk menyuplai listrik	Setiap aset harus dilindungi dari gangguan listrik dan gangguan lainnya yang disebabkan oleh kegagalan pada utilitas pendukung (9.2.2)

ID Risiko	Risiko	Kategori	Penyebab	Dampak	RPN	Level	Opsi Mitigasi	Bentuk Mitigasi	Kontrol (ISO 27001/27002)
			Hewan yang mengigit kabel listrik				Treat	Meletakkan kabel pada tempat yang tidak dapat dijangkau hewan	Setiap aset harus dilindungi dari gangguan listrik dan gangguan lainnya yang disebabkan oleh kegagalan pada utilitas pendukung (9.2.2)
			Beban listrik yang terlalu besar				Treat	Mengurangi penggunaan perangkat yang memiliki daya listrik yang besar yang tidak terlalu bermanfaat	Setiap aset harus dilindungi dari gangguan listrik dan gangguan lainnya yang disebabkan oleh kegagalan pada utilitas pendukung (9.2.2)

ID Risiko	Risiko	Kategori	Penyebab	Dampak	RPN	Level	Opsi Mitigasi	Bentuk Mitigasi	Kontrol (ISO 27001/27002)
			Hubungan arus pendek				Treat	Mengurangi penumpukan steker/colokan listrik Melakukan peemeriksaan rutin terhadap kabel listrik	Setiap aset harus dilindungi dari gangguan listrik dan gangguan lainnya yang disebabkan oleh kegagalan pada utilitas pendukung (9.2.2)

2.2.8 Manajemen Risiko TI

Menurut Valerry G Kumaat manajemen risiko merupakan tindakan terencana dan berkesinambungan untuk mengantisipasi ketidakpastian dimasa depan dengan cara mereduksi faktor-faktor yang memungkinkan terjadinya risiko, atau menekan dampak dari risiko, berdasarkan identifikasi/ observasi, pengukuran/analisis, dan penanganan/pengendalian atas faktor-faktor penyebab atau dampak risiko yang mungkin terjadi [**15**]

Menurut Stoneburner manajemen risiko merupakan serangkaian proses dalam mengidentifikasi risiko, melakukan penilaian risiko, dan menyusun serangkaian tindakan menurunkan risiko tersebut sampai level yang dapat diterima oleh organisasi [**23**]

Manajemen Risiko Teknologi Informasi (TI) adalah kemampuan organisasi dalam mengurangi risiko-risiko TI yang mungkin akan menghambat pencapaian tujuan organisasi terkait dengan pemanfaatan itu sendiri. Manajemen ririsko merupakan suatu proses pengukuran atau penilaian risiko serta pengemabangan strategi pengelolaannya [**24**]

2.2.9 Keamanan Informasi

Menurut Sarno dan Iffano (2009) Keamanan informasi adalah suatu upaya untuk mengamankan aset informasi terhadap ancaman yang timbul, sehingga keamanan informasi secara tidak langsung dapat menjamin kontinuitas bisnis, mengurangi risiko-risiko yang terjadi, mengoptimalkan pengembalian investasi (*return on investment*).

Menurut Syafrizal keamanan informasi terdiri dari perlindungan terhadap aspek-aspek berikut [**25**]:

1. Confidentiality (kerahasiaan)
   Aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh

orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.

2. Integrity (integritas)

   aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin fihak yang berwenang (authorized), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini.

3. Availability (ketersediaan)
   aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan).

Tiga elemen dasar ***confidentiality, integrity,*** dan ***availability*** (CIA) merupakan dasar diantara program program keamanan yang dikembangkan. Ketiga elemen tersebut merupakan mata rantai yang saling berhubungan dalam konsep ***information protection.***

Keamanan bisa dicapai dengan beberapa cara atau strategi yang biasa dilakukan secara simultan atau dilakukan dalam kombinasi satu dengan yang lainnya. Strategi-strategi dari keamanan informasi masing-masing memiliki fokus dan dibangun tujuan tertentu sesuai kebutuhan

2.2.10 Aset Informasi

Aset informasi merupakan bagian inti dari aset teknologi informasi. Aset informasi berisikan data dan informasi yang relevan dengan proses bisnis pada suatu organisasi. Aset Informasi pada penelitian ini meliputi komponen-komponen pendukung yang meliputi :

1. Orang (*people*)

Dalam tugas akhir ini komponen yang akan diidentifikasi adalah pengelola sistem yang ada di proses bisnis organisasi tersebut.

2. Data
   Dalam dunia teknologi informasi, yang disebut data adalah individu dari sebuah database, yang disimpan dalam basis data untuk keperluan penyediaan informasi dalam tujuannya untuk mendukung perusahaan dalam menjalankan proses operasional.
3. Perangkat Keras (*Hardware*)
   Mencakup piranti fisik, seperti computer, printer, dan monitor. Perangkat ini berperan sebagai media penyimpanan dalam system informasi. Setiap perusahaan yang memiliki teknologi informasi yang maju pasti memiliki perangksat keras dalam jumlah banyak.
4. Perangkat Lunak (*Software*)
   Merupakan sekumpulan instruksi yang dapat mempengaruhi kinerja perangkat keras dan memproses data. Tujuan perangkat ini adalah untuk mengolah, menghitung dan memanipulasi data agar menghasilkan informasi yang berguna
5. Jaringan (*Network*)
   Merupakan system penghubung yang memungkinkan suatu sumber yang digunakan bersamaan dalam waktu dan tempat yang berbeda

Kemudian komponen tersebut saling menyatu dan berinteraksi sehingga dapat berfungsi sebagai pendukung dan penyedia kebutuhan informasi dalam rangka pengambilan keputusan yang lebih baik

2.2.11 Sistem Manajemen Keamanan Informasi

Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Management System* (ISMS) adalah

sistem manajemen yang diterapkan perusahaan untuk mengamankan aset informasi terhadap ancaman yang mungkin terjadi. Oleh sebab itu, kemanan informasi secara tidak langsung menjamin kelangsungan bisnis perusahaan.

Sistem Manajemen Keamanan Informasi menjadi penting diterapkan agar informasi yang beredar di perusahaan dapat dikelola dengan benar sehingga perusahaan dapat mengambil keputusan berdasarkan informasi yang ada dengan benar pula dalam rangka memberikan layanan yang terbaik kepada pelanggan. Terdapat berbagai standar keamanan informasi yang berlaku saat ini. Yang paling banyak diterapkan adalah standar sistem manajemen informasi yang diterbitkan oleh ISO.

Sejak tahun 2005, *International Organization for Standardization* (ISO) atau Organisasi Internasional untuk Standarisasi telah mengembangkan sejumlah standar tentang Information Security Management Systems (ISMS) atau Sistem Manajemen Keamanan Informasi (SMKI) baik dalam bentuk persyaratan maupun panduan. Standar SMKI ini dikelompokkan sebagai keluarga atau seri ISO 27000 yang terdiri dari:

- ISO/IEC 27000:2014 – *ISMS Overview and Vocabulary (Third Edition)*
- ISO/IEC 27001:2013 – *ISMS Requirements (Second Edition)*
- ISO/IEC 27002:2013 – *Code of Practice for ISMS (Second Edition)*
- ISO/IEC 27003:2010 – *ISMS Implementation Guidance*
- ISO/IEC 27004:2009 – *ISMS Measurements*
- ISO/IEC 27005:2011 – *Information Security Risk Management (Second Edition)*
- ISO/IEC 27006:2015 – *ISMS Certification Body Requirements (Third Edition)*

- ISO/IEC 27007:2011 – *Guidelines for ISMS Auditing*

2.2.12 ISO 27002: 2013 Klausul Keamanan Fisik dan Lingkungan

Standar ini merupakan penamaan ulang dari ISO/IEC 17799:2005 yang berubah menjadi ISO/IEC 27002 pada Juli 2007. Standar ini dapat digunakan sebagai titik awal dalam penyusunan dan pengembangan Sistem Manajemen Keamanan Informasi (SMKI) serta dapat digunakan sebagai referensi untuk memilih control dalam proses menerapkan SMKI berdasarkan ISO/IEC 27001 [**26**]. Standar ini memberikan panduan dalam perencanaan dan implementasi suatu program untuk melindungi aset-aset informasi.

Keamanan fisik dan lingkungan membahas keamanan dari segi fisik dan lingkungan TI untuk mencegah kehilangan/kerusakan data yang diakibatkan oleh lingkungan, termasuk bencana alam dan pencurian data dalam media penyimpanan atau fasilitas informasi yang lain. Aspek yang dibahas antara lain:

a. Daerah aman
b. Peralatan keamanan
c. Pengendalian umum

ISO 27002 mempunyai beberapa *controls* dan *objectives*. Berikut ini daftar *controls* dan *objectives* pada klausul keamanan Fisik san Lingkungan yang dipaparkan pada ISO 27002 [**27**].

Tabel 2.6 Control Objective ISO 27002 Klausul Keamanan Fisik dan Lingkungan

Poin Utama	Poin Klausul	Control / Tujuan
11.1 Secure areas		Untuk mencegah akses fisik oleh pihak yang tidak

		berwenang, kerusakan dan interferensi terhadap lokasi dan informasi organisasi.
	11.1.1 Physical security perimeter	Perimeter keamanan (batasan seperti dinding, pintu masuk yang dikendalikan dengan kartu atau meja resepsionis yang dijaga) harus digunakan untuk melindungi area yang berisi informasi dan fasilitas pengolahan informasi.
	11.1.2 Physical entry controls	Area yang aman harus dilindungi dengan pengendalian entri yang sesuai untuk memastikan bahwa user yang berwenang diperbolehkan untuk mengakses
	11.1.3 Securing offices, rooms and facilities	Keamanan fisik untuk kantor, kamar, dan fasilitas harus dirancang dan diterapkan.
	11.1.4 Protecting against external and environmental	Perlindungan fisik terhadap kerusakan akibat kebakaran, banjir, gempa bumi,

	threats	ledakan, kerusuhan sipil,dan bentuk lain dari bencana alam atau buatan manusia harus dirancang dan diterapkan.
	11.1.5 Working in secure areas	Perlindungan fisik dan pedoman untuk bekerja di dalam area yang aman harus dirancang dan diterapkan.
	11.1.6 Public access, delivery and loading areas	Titik akses seperti area bongkar muat dan titik lainnya dimana orang yang tidak berwenang dapat masuk kedalam lokasi harus dikendalikan dan jika mungkin dipisahkan dari fasilitas pengolahan informasi untuk mencegah akses yang tidak berwenang
11.2 Equipment security		Untuk mencegah kehilangan, kerusakan, pencurian atau kompromi aset dan gangguan terhadap kegiatan organisasi.
	11.2.1 Equipment siting and	Peralatan harus diletakkan atau

	protection	dilindungi untuk mengurangi risiko dari ancaman lingkungan dan bahaya, dan kesempatan untuk akses yang tidak sah.
	11.2.2 Supporting utilities	Peralatan harus dilindungi dari gangguan listrik dan gangguan lain yang disebabkan oleh kegagalan dalam sarana pendukung.
	11.2.3 Cabling security	Kabel daya dan telekomunikasi yang membawa data atau mendukung layanan informasi pendukung harus dilindungi dari intersepsi atau kerusakan.
	11.2.4 Equipment maintenance	Peralatan harus dijaga/dipelihara dengan benar untuk memastikan ketersediaan dan integritasnya
	11.2.5 Removal of property	Peralatan informasi atau perangkat lunak tidak boleh dibawa keluar lokasi tanpa ijin yang berwenang
	11.2.6 Security of	Keamanan harus diterapkan pada

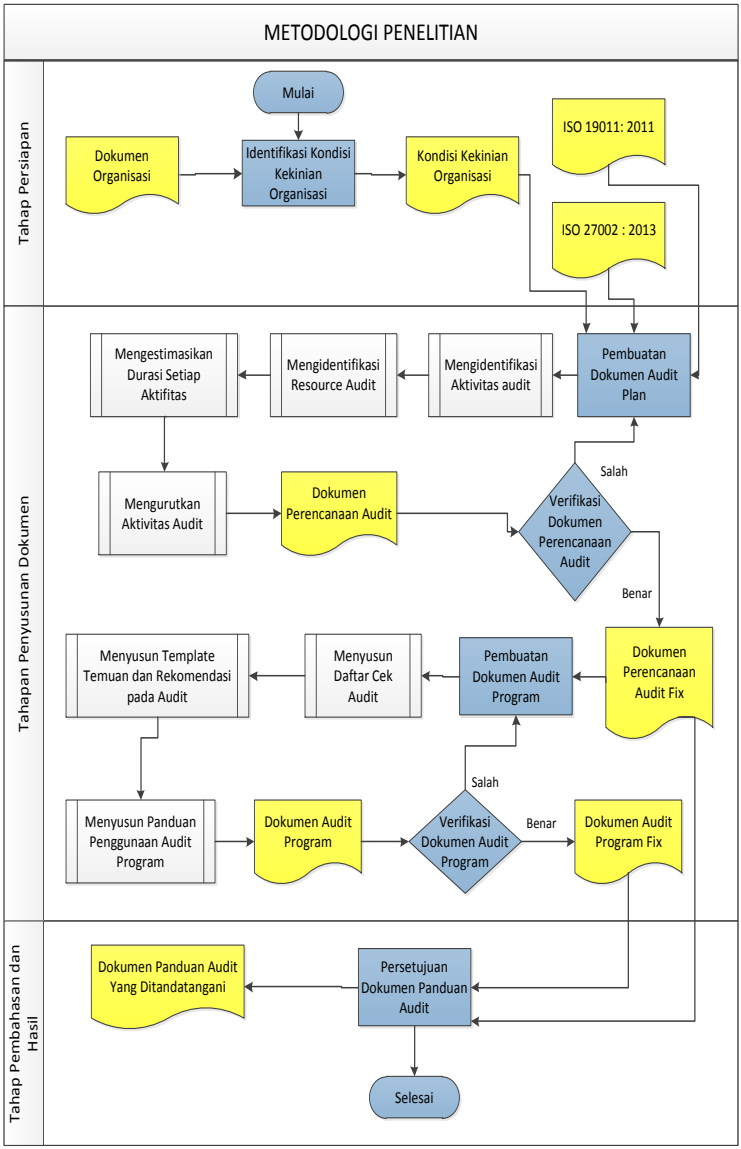
	equipment off premises	peralatan diluar lokasi dengan memperhitungkan memperhitungkan risiko yang berbeda pada saat bekerja di luar lokasi organisasi.
	11.2.7 Secure disposal or re-use of equipment	Semua item atau peralatan yang mengandung media penyimpanan harus diperiksa untuk memastikan bahwa setiap data sensitif dan perangkat lunak berlisensi telah dihapus atau ditimpa (overwritten) secara aman sebelum dibuang.
	11.2.8 Unattended User Equipment	Peralatan yang ditinggal kan 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 pengelolaan informasi harus ditetapkan

Halaman ini sengaja dikosongkan

BAB III
METODOLOGI PENELITIAN

Bab ini menjelaskan alur metode penelitian yang akan dilakukan oleh penulis dalam pembuatan tugas akhir. Metode penelitian juga digunakan sebagai panduan dalam menyelesaikan permasalahan

- Metode pengerjaan
  Metode pengerjaan yang digunakan pada tugas akhir dapat dilihat pada Gambar 3.1. Metode ini meliputi tahap persiapan, penyusunan dokumen, serta pembahasan dan hasil. Secara detail masing-masing tahapan yang akan dilewati penulis mengacu pada ISO/IEC 19011 : 2011serta metoode stepwise
- Bahan dan peralatan yang digunakan
  Berikut adalah bahan dan peralatan yang dihunakan dalam pengerjaan tugas akhir ini:
  Bahan : ISO/IEC 27002 : 2013, ISO 19011 : 2011, serta panduan dan audit program pada penelitian sebelumnya
  Peralatan : Microsoft Word, Microsoft Project, Visio



Gambar 3.1 Metode Penelitian

3.1 Tahapan Persiapan

Dalam penelitian ini, pada tahap perancangan perangkat audit merupakan tahap awal penulis melakukan aktivitas sebelum membuat perangkat audit berbasis risiko. Tahap ini harus dilakukan guna mendapat *control objective* yang akan digunakan untuk menyusun dokumen perangkat audit. Pada tahapan ini dilakukan satu tahap aktivitas, yaitu pemetaan proses dan *control objective*.

3.1.1 Mengidentifikasi Kondisi Kekinian Organisasi

Pada proses ini adalah melakukan identifikasi kondisi kekinian yang ada di organisasi. Inputan dari proses ini adalah melakukan observasi terhadap dokumen organisasi terkait visi misi, struktur organnisasi serta tugas dan fungsinya. Output dari proses ini adalah visi dan misi, struktor organisasi serta tugas dan fungsi auditee yang akan bertanggung jawab pada proses audit.

3.2 Tahap Penyusunan Dokumen

3.2.1 Penyusunan Audit Plan

- **Mengidentifikasi Aktifitas**

Mengidentifikasi aktifitas merupakan proses pertama pada tahap ini yaitu mengidentifikasi aktifitas. Inputan proses ini adalah *control objective* yang telah ditentukan pada penentuan ruang lingkup yaitu terkait keamanan fisik dan lingkungan. Teknik yang dipakai dalam mengidentifikasi aktifitas adalah dengan menganalisa *implementation guidance* pada semua *control objective* terkait keamanan fisik dan lingkungan. Outputnya yang akan dihasilkan adalah aktifitas aktifitas Audit.

- **Menentukan Resource pada Setiap Aktifitas**

Pada sub proses ini dilakukan proses observasi pada dokumen organisasi yaitu pada dokumen tugas dan fungsi pada struktur organisasi. Dalam bagian ini dijelaskan bagaimana menyesuaikan rencana aktifitas dengan ketersediaan sumberdaya yang ada. Pengalokasian Resource pada aktifitas nantinya akan merubah rencana aktifitas yang ideal. Sehingga output pada sub proses adalah WBS yang telah terupdate dengan sumberdaya yang akan dipakai.

- **Mengestimasikan Durasi Setiap Aktifitas**

Inputan dari proses ini adalah daftar aktivitas yang telah dilakukan pada sub-proses sebelumnya. Untuk mengestimasikan durasi setiap aktifitas dilakukan dengan cara melakukan analisisa menggunakan teknik parametrik. Luaran dari sub proses ini adalah daftar aktifitas yang diestimasikan durasinya.

- **Mengurutkan Aktifitas**

Pada sub-proses ini adalah mengurutkan aktivitas yang telah diidentifikasi pada sub-proses sebelumnya yaitu dengan mengelompokkan aktifitas berdasarkan resource yang telah ditentukan . Sub-proses ini bertujuan untuk mengefisiankan waktu pada saat melakukan proses audit. Luaran dari proses ini adalah WBS yang terupdate dengan urutan aktifitas yang baik.

3.2.2 Verifikasi Dokumen Perencanaan Audit

Proses selanjutnya adalah melakukan verifikasi dokumen Perencanaan Audit yang telah dibuat pada proses selanjutnya. Pada proses ini bertujuan untuk mengetahui apakah setiap poin dari dari dokumen yang telah disusun pada Perencanaan Audit sudah benar.

Proses verifikasi yang dilakukan terlebih dahulu adalah proses verifikasi yang akan dilakukan oleh pihak IS-NET terkait informasi yang diminta oleh penulis pada dokumen

perencanaan audit. Selanjutnya untuk poin-poin yang lain akan ditiinjau ulang dengan dokumen lain yang terkait.

Apabila dalam dokumen Perencanaan Audit yang diverifikasi terdapat kesalahan maka penulis akan memperbaiki dokumen dengan mengulang proses sebelumnya. Output dari proses ini adalah dokumen *audit plan* yang telah diverifikasi

3.2.3 Menyusun Dokumen Audit program

Proses ini merupakan proses akhir pada tahap ini, dalam penyusunan dokumen *audit program* ini nantinya akan menghasilkan dokumen audit program, dalam proses ini penulis membagi beberapa sub proses yaitu sebagai berikut:

- **Menyusun Daftar Cek Audit**
  Pada sub proses ini akan membuat daftar check audit atau *audit checklist* untuk setiap prosedur yang telah dibuat pada sub proses sebelumnya. Daftar cek audit berisikan bagaimana melakukan suatu prosedur audit, status dari komponen yang dicek (apakah sesuai, tidak sesuai, ataukah parsial), dan bukti dari pemberian status dari komponen yang dicek. Daftar cek audit dapat berisi pengujian *compliance* atau *substantive test* dari Pengelolaan di IS-Net.

- **Penyusunan *template* Temuan dan Rekomendasi pada Audit**
  pada sub proses ini akan dibuatkan *template* untuk temuan dan rekomendasi dari audit yang mengacu pada penelitian-penelitian sebelumnya. Template ini nantinya akan berisi rangkuman hasil audit dan menuliskan rekomendasi apa saja yang harus dilakukan untuk memperbaiki hal yang tidak sesuai dengan kontrol klausul kemanan fisik dan lingkungan, juga berisi siapa yang bertanggung jawab, serta kapan batas akhir dalam menyelesaikan perbaikan tersebut.

- **Penyusunan Panduan Penggunaan Audit Program**
  Pada sub proses ini akan membuat panduan penggunaan audit program yang telah dibuat sebelumnya. Panduan tersebut menjelaskan tiap komponen yang ada pada *audit program*, penjelasan penggunaan tiap dokumen audit program (kapan dan siapa yang menggunakan), serta petunjuk bagaimana mengisi *audit program.* Dengan adanya panduan ini diharapkan pihak JSI dapat menggunakan *audit program* dengan baik sesuai dengan yang ada pada panduan ini.

3.2.4 Melakukan Verifikasi Dokumen Audit Program

Proses ini merupakan proses dimana penulis akan melakukan verifikasi verifikasi terhadap audit program yang telah dibuat sebelumnya.

- Verifikasi ini yaitu melakukan pengecekan apakah Audit Program yang dibuat telah sesuai dengan kontrol acuan yang digunakan dengan cara melakukan *trace back* atau penelusuran kembali pada tiap prosedur audit dan daftar cek audit apakah telah sesuai dengan kontrol keamanan fisik dan lingkungan yang ada pada ISO/IEC 27002:2013. Kemudian juga melakukan pengecekan untuk mengetahui apakah kontrol pada klausul kemanan fisik dan lingkungan telah digunakan untuk aktifitas dan *audit checklist*. Dilanjutkan dengan melakukan verifikasi *audit checklist* kepada pihak IS-NET dengan maksud untuk mengetahui apakah *audit checklist* yang dibuat dapat dimengerti dan dipahami oleh pihak IS-NET sehingga nantinya tidak akan menimbulkan pertanyaan terkait *audit checklist.*
- Kemudian melanjutkan untuk memverifikasi panduan penggunaan dokumen *audit program* yang dibuat dengan cara melakukan tinjauan ulang apakah penjelasan-penjelasan yang ada pada panduan tersebut telah sesuai dengan fungsinya serta dapat dimengerti oleh penggunanya.

- Apabila dalam dokumen *audit program* yang diverifikasi terdapat kesalahan maka penulis akan memperbaiki dokumen dengan mengulang proses sebelumnya. Output dari proses ini adalah dokumen *audit program* yang telah diverifikasi.

3.3 Tahapan Pembahasan dan Hasil

Tahap kedua dalam pengerjaan penelitian ini adalah tahap analisis risiko. Pada tahap ini, penulis melakukan dua tahapan proses diantaranya adalah tahap mengumpulkan data terkait risiko dan tahap menganalisis risiko.

3.3.1 Persetujuan Dokumen Panduan Audit

Selanjutnya adalah proses persetujuan dokumen panduan audit dimana proses ini merupakan proses akhir dari keseluruhan metodologi dimana penulis melakukan proses persetujuan terhadap dokumen panduan audit yang telah dibuat. Dokumen panduan audit yang berisi audit plan dan audit program akan ditanda tangani dan siap digunakan oleh pihak IS-NET.

Halaman ini sengaja dikosongkan

BAB IV
PERANCANGAN

Bagian ini menjelaskan mengenai perancangan penulisan tugas akhir yang dilakukan. Perancangan ini bertujuan untuk menjadi panduan dalam melakukan penulisan tugas akhir.

4.1 Perancangan Studi Kasus

4.2.1 Tujuan Studi Kasus

Pada penelitian ini akan dilakukan pembuatan dokumen Panduan Audit berdasarkan ISO/IEC 27002:2013 sebagai acuan dalam membuat audit programnya, sedangkan dalam menysusun dokumen audit plannya mengacu pada PMBOK supaya dalam menyusun panduan auditnya tersusun dengan baik dan tidak dilakukan dengan sembarangan. Dalam melakukan penelitian ini diperlukan sebuah studi kasus sebagai lokasi pengimplementasian panduan audit dalam melakukan kegiatan audit. Penggunaan studi kasus memungkinkan peneliti untuk meneliti data dalam konteks tertentu. Studi kasus dalam penelitian merupakan sebuah aktivitas pengamatan yang berfokus untuk mendeskripsikan, memahami, memprediksi atauupun mengontrol sebuah individu [1]. Sedangkan Menurut Yin jika menggunakan studi kasus dalam penelitian, peneliti dapat menggali lebih dalam menggunakan konteks kehidupan nyata dengan berbagai macam cara yang sistematis dalam pengumpulan data seperti wawancara dan observasi [**28**]. Yin menjelaskan terdapat tiga tipe dari studi kasus antara lain :

- *Exploratory* (eksplorasi)
  Studi kasus eksplorasi yakni melakukan eksplorasi terhadap fenomena apapun dalam data yang berfungsi sebagai tempat tujuan untuk peneliti.
- *Descriptive* (Deskriptif)

Studi kasus deskripsi yakni menggambarkan fenomena ilmiah yang terjadi dalam data yang dimaksud. Tujuan dari studi kasus ini yakni menggambarkan data yang terjadi dalam bentuk narasi.

- *Explanatory* (memperjelas)
  Studi kasus memperjelas yakni menjelaskan fenomena dalam data secara jelas dan detail.

Dalam penelitian ini dirancang dengan menggunakan studi kasus. Penggunaan studi kasus dalam pengerjaan penelitian ini adalah untuk melakukan eksplorasi suatu permasalahan lebih mendalam lagi. Harapan penlitian dengan menggunakan studi kasus adalah untuk mempermudah penggalian informasi dan penerapan data.
Dalam melakukan sebuah penelitian menurut Yin langkah yang dapat dilakukan adalah melakukan perancangan penelitian. Pada proses perancangan inilah yang nantinya akan membantu penulis dalam menentukan dan memahami tujuan studi kasus, persiapan pengumpulan data untuk kebutuhan penulisan, persiapan pengumpulan data untuk kebutuhan penelitian,menentukan metode pengolahan data hingga menentukan pendekatan untuk melakukan analisis mendalam mengenai data yang nantinya akan digunakan selama proses penelitian.

4.2.2 Unit Of Analysis

Perancangan studi kasus dapat dilakukan dengan menggunakan dua macam tipe yaitu :

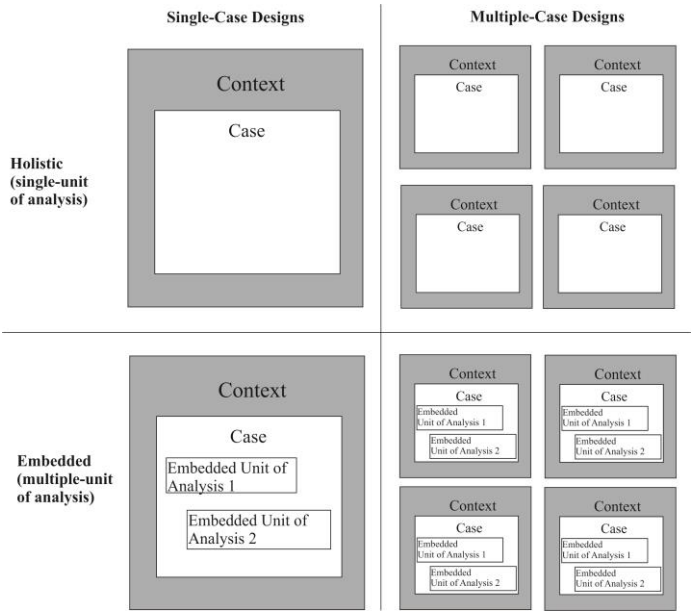
- *Single-case design*
  Pada tipe studi kasus ini menggunakan hanya satu studi kasus untuk diuji. *Single-case* digunakan dalam penelitian untuk melakukan pengujian lebih lanjut terhadap teori yang telah dirumuskan.
- *Multiple-case design*

> Pada tipe studi kasus ini menggunakan dua atau lebih dari dua kasus yang diuji. *Multiple-case* digunakan pada jenis penelitian yang membutuhkan eksplorasi perbedaan pada masing-masing studi kasus yang dieksplorasi.

Terdapat dua *unit of analysis* dari tipe perancangan studi kasus tersebut yaitu *Holistic (single unit of analysis)* yang hanya terdapat satu analisis unit dan *Embedded* yang terdapat lebih dari satu analisis unit. Sehingga terdapat empat macam desain dasar pada sebuah studi kasus yakni :

1. *Single case-holistic*
2. *Single case-Embedded*
3. *Multiple-Holistic*
4. *Multiple-Embedded*

Dalam memilih studi kasus terdapat dua tipe yaitu *single-case design* dan *multiple-case design.* Terdapat perbedaan diantara kedua tipe tersebut jika digunakan dalam suatu penulisan, *Single-case design* merupakan tipe perancangan studi kasus dengan menggunakan pengujian pada satu studi kasus sehingga dapat mengeksplorasi lebih lanjut terhadap metode yang digunakan di dalamnya. *Single-case design* banyak digunakan pada penulisan dengan kasus yang unik, kritis, menguji kebenaran suatu teori, mengamati dan mengeksplorasi kondisi tertentu pada suatu kasus. Tipe yang kedua adalah *multiple-case design* dimana tipe ini menggunakan lebih dari satu studi kasus yang bertujuan untuk membandingkan beberapa studi kasus yang ada dan bertujuan untuk melakukan replikasi temuan di seluruh studi kasus. Perbedaan mendasar kedua tipe ini terletak pada jumlah *unit of analysis* yang digunakan seperti yang dapat terlihat pada Gambar 4.1 Type Unit Of Analysis [**28**].



Gambar 4.1 Type Unit Of Analysis (Book: A Case Study Methodology)

Pada tugas akhir ini digunakan tipe perancangan studi kasus *single-case design-holistic*. Tipe perancangan studi kasus *single-case design-holistic* karena penulis akan mengeksplorasi sebuah permasalahan dalam sebuah studi kasus yaitu penyususnan dokumen panduan audit pada Objek Penelitian.

4.2 Persiapan Pengumpulan Data

Persiapan pengumpulan data merupakan tahapan yang ada pada tahapan perancangan. Di dalam bagian ini akan dibahas bagaimana metode yang akan digunkan dalam pengumpulan data pada stusi kasus penulisan. Menurut said (2015) mengatakan dalam artikelnya, teknik pengumpulan data pada penulisan terdapat 5 teknik diantaranya adalah kuesioner, tes,

wawancara, dokumen, dan observasi. Beberapa metode di atas akan digunakan dalam jangka waktu tertentu selama proses penulisan berlanngsusng sesuai dengan kerangka kerja yang diterapkan pad astudikasus untuk mencapai suatu tuuan yang diinginkan.

Dalam mengumpulkan data yang dibutuhkan penulis menggunakan metode observvasi. Dalam penggalian data dengan menggunakan proses wawancara penulis melakukan wawancara terhadap orang yang berhubungan dengan dengan pihak yang bertanggung jawab dalam pengelolaan ruang server yaitu sekretaris jurusan sistem informasi. Kegiatan wawancara yang akan dilakukan bertujuan untuk mendapatkan informasi kekinian organisasi, audit yang pernah dilakukan serta siapa saja auditor dan auditee yang nantinya akan melakukan kegiatan audit. Metode yang kedua adalah melakukan riview dokumen sebelumnya yaitu dengan cara melihat dokumen *risk register* serta dokumen audit program yang pernah dibuat sebelumnya sehingga informasi tersebut dapat dijadikan acuan yang dapat membantu penulis dalam pembuatan panduan audit. Sedangkan metode yang terakhir adalah melakukan observasi terhadap ruang server atau IS-NET guna untuk mengetahui bagaimana pengelolaan keamanan fisik dan lingkungan TI di area IS-NET. Dari ketiga metode pengumpulan data akan dilakukan dalam penelitian ini, berikut beberapa detail data yang ingin di dapatkan selama proses penelitian:

1. Kondisi Kekinian Organisasi
2. Tugas pokok dan fungsi unit di IS-NET

4.3 Metode Pengolahan Data

Metode pengolahan data pada penulisan ini terdapat dua metode yang digunakan. Metode pertama dilakukan agar penulis dapat dengan mudah melakukan analisis pada hasil

wawancara dengan narasumber, yaitu data dari hasil wawancara yang telah direkam menggunakan bantuan alat perekam kemudian disalin pada aplikasi *Microsoft Word*. Setelah data disalin dan disimpan di aplikasi *Microsoft Word*, data akan lebih mudah untuk diolah seperti melakukan *highlight text*, *underline point*, hingga menerjemahkan hasil wawancara narasumber dalam sebuah kalimat. Metode pengolahan data yang digunakan yaitu dengan cara melakukan analisis deskriptif dari data yang didapatkan dengan memaparkannya ke dalam tabel sehingga data menjadi lebih mudah untuk dipahami. Sedangkan data yang didapatkan melalui observasi dilakukan pencatatan terhadap hasil pengamatan tersebut.

4.4 Pendekatan Analisis

Pada Bagian ini akan menjelaskan pendekatan analisis yang akan digunakandalam penelitian tugas akhir. Analisis ini dilakukan untuk mengetahui hubungan antara data yang didapat dan akan menggunakannya pada tahapan pengerjaan penulisan. Beberapa pendekatan analisis yang akan dilakukan antara lain adalah:

a. **Analisis kondisi kekinian pengelolaan ruang server**
   Analisis ini dilakukan untuk mengetahui kondisi kekinian pengelolaan ruang server serta risiko-risko yang ada terhadap keamanan fisik dan lingkungan yang nantinya akan dipetakan dalam standar ISO/IEC 27002:2013 untuk menetapkan ruang lingkup yang nantinya akan dijadikan acuan dalam membuat perangkat audit.

b. Analisis dengan pendekatan standar acuan

   a. PMBOK – *Project Plan*
      Analisis dengan PMBOK pada proses *project plan* digunakan untuk menganalisis hal yang diperlukan saat akan menyususn dokumen *audit plan.*

b. *ISO* 19011:2011 – Audit
   Analisis dengan menggunakan ISO 19011:2011 digunakan untuk menganalisis aktifitas-aktifitas yang akan dilakukan dalam kegiatan audit yang disusun dalam *audit plan.*
c. ISO 27002:2013 – Keamanan Fisik dan lingkungan TI

Analisis dengan ISO/IEC 27002:2013 pada klausul keamanan fisik dan lingkungan digunakan untuk mengetahui kendali tujuan apa saja yang dipakai dalam praktik keamanan fisik dan lingkungan yang sesuai dengan standar

Halaman ini sengaja dikosongkan

BAB V
IMPLEMENTASI

Bab ini menjelaskan mengenai hasil implementasi yang diperoleh dari proses perancangan pada bab IV yang telah dijabarkan sebelumnya. Hasil implementasi akan berupa data dan informasi mentah.

5.1 Kondisi Kekinian Organisasi

Visi

Visi Jurusan Sistem Informasi Tahun adalah menjadi Jurusan Sistem Informasi berbasis riset bereputasi internasional pada tahun 2025.

Misi

Misi Jurusan Sistem Informasi Tahun mencakup aspek pendidikan, penelitian, dan pengabdian masyarakat (Tridharma Perguruan Tinggi), yakni:

1. Menyelenggarakan pendidikan tinggi yang berkualitas di bidang Sistem Informasi
2. Mengembangkan dan menerapkan sistem informasi/teknologi informasi yang mensejahterakan masyarakat dan meningkatkan daya saing bangsa.
3. Memberikan kepuasan dan kesejahteraan kepada setiap sivitas Sistem Informasi.

Nilai

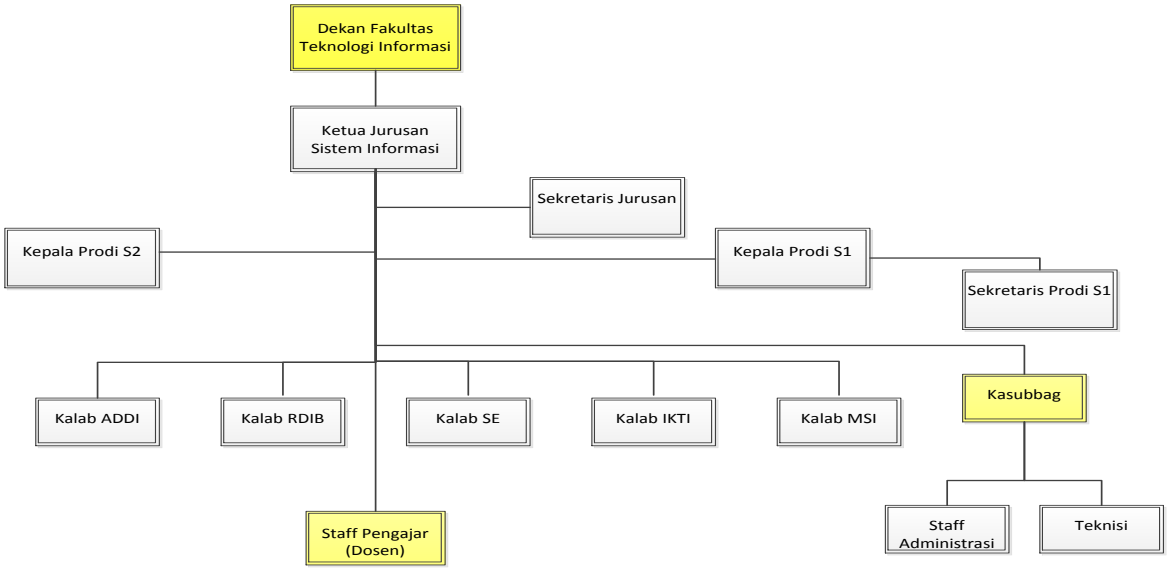
Nilai-nilai yang ingin ditanamkan oleh Jurusan Sistem Informasi adalah:

1. **Etika dan Integritas** *(Ethics and Integrity)*; dalam kehidupan bermasyarakat, bernegara, maupun menjalankan profesinya, selalu berpegang teguh pada norma-norma dan peraturan-peraturan yang berlaku di masyarakat, negara, dan agama.

2. **Kreativitas dan Inovasi** *(Creativity and Innovation)*; selalu mencari ide-ide baru untuk menghasilkan inovasi dalam menjalankan tugas/perannya dengan lebih baik.
3. **Ekselensi** *(Excellence)*; berusaha secara maksimal untuk mencapai hasil yang sempurna.
4. **Kepemimpinan yang kuat** *(Strong Leadership)*; menunjukkan perilaku yang visioner, kreatif, inovatif, pekerja keras, berani melakukan perubahan-perubahan ke arah yang lebih baik, dan bertanggung jawab.
5. **Sinergi** *(Synergy)*; bekerja sama untuk dapat memanfaatkan semaksimal mungkin potensi yang dimiliki.
6. **Kebersamaan Sosial dan Tanggung Jawab Sosial** (Socio-cohesiveness and Social Responsibility); menjaga kerukunan dan peduli terhadap masyarakat sekitar.

5.2 Struktur Organisasi Jurusan Sistem Informasi

Berdasarkan observasi terhadap dokumen yang ada berikut adalah struktur organisasi yang ada di Jurusan Sistem Informasi yang akan dipaparkan pada gambar 5.1.



Gambar 5.1 Struktur Organisasi Jurusan Sistem Informasi

5.3 Tugas Dan Fungsi Auditee

Berdasarkan observasi terhadap dokumen tugas dan fungsi yang dimiliki oleh jurusan sistem informasi, dapat ditentukan 3 orang auditee yang nantinya akan bertanggung jawab memberikan penjelasan serta ketersediaan dokumen yang ada yang berkaitan dengan IS-Net saat pelaksanaan audit berlangsung. Tabel 5.1 sampai tabel 5.3 memberikan penjelasan mengenai tugas dan fungsi ketiga auditee yaitu:

1. Pengadministrasian BMN
2. Teknisi Sarpras Listrik
3. Teknisi Sarpras SI/TI

Tabel 5.1 Tugas dan Fungsi Pengadministrasian BMN

Rumusan Tugas Peangadministrasian BMN
Menerima, mencatat dan memproses barang milik negara (BMN) sesuai dengan ketentuan dan peraturan yang berlaku;
Rincian Tugas
1. Menerima dan memeriksa BMN sesuai dengan prosedur; - Menjadi panitia penerima pengadaan barang dan jasa 2. Mencatat BMN ke dalam buku induk BMN; - Menerima dan mencatat barang habis pakai ke kartu barang - Mengentry data ke SIMAK persediaan - Mencatat barang habis pakai 3. Membuat kode inventaris BMN sesuai dengan ketentuan; - Membuat daftar inventaris ruangan 4. Mendistribusikan BMN ke bagian terkait; 5. Memberikan layanan permintaan dan peminjaman BMN sesuai dengan prosedur; 6. Menginventarisir BMN sesuai dengan ketentuan;

- Memberi label BMN 7. Menata BMN sesuai dengan prosedur; 8. Menghitung persediaan jumlah dan kondisi BMN; - Melakukan stock opname BMN setiap semester 9. Menyiapkan bahan usul penghapusan BMN; 10. Menyimpan arsip dan dokumen BMN; 11. Melaporkan pelaksanaan tugas kepada atasan sebagai pertanggungjawaban pelaksanaan; - Melakukan entry data barang inventaris ke SIM Keuangan - Membuat laporan bulanan barang habis pakai 12. Melaksanakan tugas kedinasan lain yang diperintahkan oleh pimpinan.
Hasil kerja
1. Pemeriksaan BMN; 2. Catatan BMN dalam buku induk BMN; 3. Kode inventaris BMN; 4. Pendistribusian BMN ke unit terkait; 5. Layanan permintaan dan peminjaman BMN; 6. Inventarisasi BMN; 7. Penataan BMN; 8. Perhitungan persediaan jumlah dan kondisi BMN; 9. Bahan usul penghapusan BMN; 10. Penataan arsip dan dokumen BMN; 11. Laporan hasil pelaksanaan tugas; 12. Pelaksanaan tugas kedinasan lain.

Tabel 5.2 Tugas dan Fungsi Teknisi Sarpras Listrik

Rumasan Tugas Teknisi Sarpras Listrik
Melakukan perawatan, pemeliharaan dan perbaikan sarana dan prasarana kelistrikan kantor sesuai dengan ketentuan untuk mendukung operasional kantor.

Rincian Tugas
1. Menyiapkan sarana dan prasarana (Listrik, Genset, AC dan Alat Musik) untuk kegiatan akademik perkuliahan dan operasional kantor; 2. Melakukan instalasi listrik di kantor; 3. Memeriksa kondisi sarana dan prasarana kantor (Listrik, Genset, AC dan Alat Musik)sebagai bahan perawatan dan perbaikan; 4. Melaksanakan perawatan dan pemeliharaan sarana dan prasarana kantor (Listrik, Genset, AC dan Alat Musik) secara berkala; 5. Memperbaiki sarana dan prasarana kantor (Listrik, Genset, AC dan Alat Musik) yang rusak sesuai dengan ketentuan; 6. Menyusun laporan perbaikan sebagai bahan penanganan lebih lanjut; 7. Melayani peminjaman sarana prasarana (Listrik, Genset, AC dan Alat Musik) untuk kegiatan operasional unit terkait; 8. Melayani keluhan pengguna (Listrik, AC dan Alat Musik) di kantor; 9. Menginventarisasi dan melaporkan barang dan peralatan (Listrik, Genset, AC dan Alat Musik) yang tersedia; 10. Melakukan kontrol ketersediaan air di kantor; 11. Melaporkan hasil pelaksanaan tugas kepada atasan sebagai pertanggungjawaban; 12. Melaksanakan tugas kedinasan lain yang diberikan atasan.
Hasil kerja
1. Kesiapan fasilitas (Listrik, Genset, AC dan Alat Musik) untuk kegiatan akademik dan operasional; 2. Tersedianya instalasi listrik; 3. Catatan kondisi sarana dan prasarana kantor (Listrik, Genset, AC dan Alat Musik); 4. Perawatan dan pemeliharaan secara berkala;

5. Perbaikan sarana dan prasarana kantor (Listrik, Genset, AC dan Alat Musik); 6. Laporan perbaikan; 7. Layanan peminjaman sarana dan prasarana kantor (Listrik, Genset, AC dan Alat Musik); 8. Penanganan terhadap keluhan pengguna (Listrik, Genset, AC dan Alat Musik); 9. Catatan inventarisasi dan laporan stock opname barang dan peralatan SI/TI; 10. Ketersediaan air di kantor; 11. Laporan hasil pelaksanaan tugas; 12. Laporan hasil pelaksanaan tugas kedinasan lain.

Tabel 5.3 Tugas dan Fungsi Teknisi Sarpras SI/TI

Rumusan Tugas Peangadministrasian BMN
Melakukan perawatan, pemeliharaan dan perbaikan sarana dan prasarana SI/TI kantor sesuai dengan ketentuan untuk mendukung operasional kantor.
Rincian Tugas
1. Menyiapkan fasilitas SI/TI untuk kegiatan akademik perkuliahan dan operasional kantor; 2. Melakukan instalasi perangkat lunak seperti server Web, server switch/router, hotspot, SITV; 3. Melakukan instalasi perangkat keras jaringan dan komputer; 4. Memeriksa kondisi sarana dan prasarana SI/TI kantor sebagai bahan perawatan dan perbaikan; 5. Melaksanakan perawatan dan pemeliharaan sarana dan prasarana SI/TI kantor secara berkala; 6. Memperbaiki sarana dan prasarana SI/TI kantor yang rusak sesuai dengan ketentuan; 7. Menyusun laporan perbaikan sebagai bahan penanganan lebih lanjut;

8. Melayani peminjaman sarana prasarana SI/TI untuk kegiatan operasional unit terkait; 9. Melayani keluhan pengguna SI/TI di kantor; 10. Menginventarisasi dan melaporkan barang dan peralatan SI/TI yang tersedia; 11. Melaporkan hasil pelaksanaan tugas kepada atasan sebagai pertanggungjawaban; 12. Melaksanakan tugas kedinasan lain yang diberikan atasan.
Hasil kerja
1. Kesiapan fasilitas SI/TI untuk kegiatan akademik; 2. Tersedianya server Web, server switch/router, hotspot dan SITV 3. Tersedianya jaringan internet dan komputer; 4. Catatan kondisi sarana dan prasarana kantor; 5. Perawatan dan pemeliharaan secara berkala; 6. Perbaikan sarana dan prasarana kantor; 7. Laporan perbaikan; 8. Layanan peminjaman sarana dan prasarana kantor; 9. Penanganan terhadap keluhan pengguna SI/TI; 10. Catatan inventarisasi dan laporan stock opname barang dan peralatan SI/TI; 11. Laporan hasil pelaksanaan tugas; 12. Laporan hasil pelaksanaan tugas kedinasan lain.

5.4 Penyusunan Audit Plan

5.4.1 Mengidentifikasi Aktifitas

Pengidentifikasian aktifitas ini adalah tahap awal dalam membuat audit plan, dikarenakan aktifitas adalah bagian utama dari sebuah rencana. Inputan yang dipakai pada proses ini adalah semua control objective yang ada pada klausul keamanan fisik dan lingkungan. Untuk mendapatkan aktifitas diperlukan untuk melakukan analisa terhadap implementation guidance pada semua control objective. Tabel berikut merupakan proses analisa sehingga menghasilkan aktifita-aktifitas audit:

Tabel 5.4 Penentuan Aktifitas audit pada Control objective 11.1.1

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**
Control Objective	***Implementation Guidance***	
11.1.1 *Physical Security Perimeter*	a. perimeter (denah) keamanan harus didefinisikan, dan peletakan dan kekuatan dari masing-masing perimeter harus didasarkan pada kebutuhan keamanan aset dalam perimeter dan hasil penilaian risiko;	1. Auditor menanyakan kepada pengadministrasian BMN terkait adanya kebutuhan perimeter (denah) untuk melindungi aset 2. Auditor menanyakan kepada Pengadministrasian BMN terkait pendefinisian perimeter (denah) keamanan pada ruang server 3. Auditor melakukan cek ketersediaan pendefinisan letak dalam denah bangunan ruang server 4. Auditor melakukan cek ketersediaan pendefinisian konstruksi dalam denah bangunan ruang server 5. Auditor melakukan cek kesesuaian letak bangunan ruang server dengan denah

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
		bangunan ruang server 6. Auditor melakukan cek kesesuaian konstruksi bangunan dengan denah bangunan ruang server
	b. bangunan atau tempat yang berisi fasilitas pengolahan informasi secara fisik harus kedap suara ; atap eksterior, dinding dan lantai dari bangunan harus dari konstruksi yang solid dan semua pintu eksternal harus dilindungi terhadap akses yang tidak sah sesuai dengan mekanisme kontrol, (misalnya alarm dan kunci); pintu dan jendela luar harus terkunci ketika ruangan ditinggalkan;	7. Auditor melakukan cek terhadap bangunan terkait adanya celah pada bangunan 8. Auditor melakukan cek pada konstruksi atap, dinding dan lantai terkait konstruksi yang dipakai 9. Auditor melakukan cek pada pintu luar ruang server terkait adanya pengamanan akses masuk 10. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur penguncian pintu dan jendela luar ketika ditinggalkan

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
	c. area resepsionis atau cara lain untuk mengendalikan akses fisik ke lokasi atau bangunan harus di tempat; akses ke tempat dan bangunan harus dibatasi hanya untuk orang untuk orang yang berwenang saja	11. Auditor melakukan cek terkait adanya area resepsionis 12. Auditor menanyakan kepada teknisi sarpras SI/TI terkait tersedianya daftar orang yang boleh masuk keruang server
	d. penghalang fisik harus, dibangun untuk mencegah akses fisik tidak sah dan pencemaran lingkungan;	13. Auditor melakukan cek terkait adanya batasan fisik ruang server dengan ruangan lain
	e. semua pemicu kebakaran pada bangunan harus diperhitungkan, dipantau dan diuji; dalam membangun dinding harus didasarkan dengan standar regional, nasional dan	14. Auditor menanyakan kepada pengadministrasian BMN terkait adanya standar yang yang diacu dalam memilih konstruksi yang anti api 15. Auditor melakukan cek kesesuaian konsruksi bangunan dengan standar yang

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
	internasional yang sesuai;	diacu
	f. Sistem pendeteksi penyusup yang cocok harus dipasang dan secara teratur diuji yang mencakup pintu dan jendela yang mungkin diakses; daerah kosong harus diamankan	16. Auditor memeriksa ketersediaan alat pendeteksi penyusup di ruang server 17. Auditor menanyakan kepada pengadministrasian BMN terkait adanya standar yang yang diacu dalam memilih alat pendeteksi 18. Auditor menanyakan kepada pengadministrasian BMN terkait adanya daftar spesifikasi alat pendeteksi 19. Auditor melakukan cek kesesuaian daftar spesifikasi alat pendeteksi penyusup dengan standar yang ada 20. Auditor melakukan cek ketersediaan ruang computer diruang server
	g. Fasilitas pengolahan informasi yang dikelola oleh organisasi	21. Auditor melakukan cek terkait pemisahan fasilitas pengolahan informasi

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
	harus secara fisik dipisahkan dari yang dikelola oleh pihak eksternal	secara fisik yang dikelola oleh organisasi dengan pihak eksternal

5.4.2 Menentukan Resource Setiap Aktifitas

Setelah mengidentifikasi aktifitas untuk membuat sebuah audit plan dibutuhkan resource yang bertanggung jawab (auditee) setiap aktifitas, sehingga nantinya dapat memudahkan auditor dalam menjalankan aktifitas audit. Dalam penentuan resource diperlukan inputan struktur organisasi, tugas dan fungsi yang ada pada struktur organisasi tersebut serta aktifitas yang telah diidentifikasi sebelumnya. Hasil dari proses ini adalah daftar aktifitas audit yang telah memiliki resource (auditee). Berikut adalah hasil penentuan resource setiap aktifitas berdasarkan tupoksi yang telah dijelaskan pada bab sebelumnya.

Tabel 5.5 Menentukan Resource Setiap Aktifitas pada Control Objective 11.1

No	Aktifitas Audit	Resourece
1	Auditor menanyakan kepada Pengelola administrasi BMN terkait adanya kebutuhan perimeter untuk melindungi aset	Pengelola administrasi BMN
2	Auditor menanyakan kepada Pengelola administrasi BMN terkait pendefinisian perimeter keamanan pada ruang server	Pengelola administrasi BMN
3	Auditor melakukan cek ketersediaan letak perimeter dalam dokumen arsitektur bangunan ruang server	Pengelola administrasi BMN
4	Auditor melakukan cek kesesuaian letak bangunan ruang server dengan dokumen arsitektur bangunan	Teknisi sarpras SI/TI
5	Auditor melakukan cek ketersediaan pendefinisian konstruksi perimeter dalam dokumen arsitektur bangunan ruang server	Pengelola administrasi BMN
6	Auditor melakukan cek kesesuaian konstruksi bangunan dengan dokumen arsitektur bangunan	Teknisi sarpras SI/TI
7	Auditor melakukan cek terhadap bangunan terkait adanya celah pada bangunan	Teknisi sarpras SI/TI
8	Auditor melakukan cek pada konstruksi atap, dinding dan lantai	Teknisi sarpras SI/TI
9	Auditor melakukan cek pada pintu luar ruang server terkait adanya pengamanan akses masuk	Teknisi sarpras SI/TI
10	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur penguncian pintu dan jendela eksternal ketika ditinggalkan	Teknisi sarpras SI/TI Teknisi sarpras SI/TI

No	Aktifitas Audit	Resourece
11	Auditor melakukan cek terkait adanya area resepsionis	Teknisi sarpras SI/TI
12	Auditor menanyakan kepada teknisi sarpras SI/TI terkait daftar orang yang boleh masuk keruang server	Teknisi sarpras SI/TI
13	Auditor melakukan cek terkait adanya batasan fisik dengan ruangan lain	Teknisi sarpras SI/TI
14	Auditor menanyakan kepada Pengelola administrasi BMN terkait adanya standar yang yang diacu dalam memilih konstruksi yang anti api	Pengelola administrasi BMN
15	Auditor melakukan cek kesesuaian konsruksi bangunan dengan standar yang diacu	Teknisi sarpras SI/TI
16	Auditor memeriksa ketersediaan alat pendeteksi penyusup di ruang server	Teknisi sarpras SI/TI
17	Auditor menanyakan kepada Pengelola administrasi BMN terkait adanya standar yang yang diacu dalam memilih alat pendeteksi	Pengelola administrasi BMN
18	Auditor menanyakan kepada Pengelola administrasi BMN terkait adanya daftar spesifikasi alat pendeteksi	Pengelola administrasi BMN
19	Auditor melakukan cek kesesuaian daftar spesifikasi alat pendeteksi penyusup dengan standar yang ada	Teknisi sarpras SI/TI
20	Auditor melakukan cek ketersediaan ruang komputer	Teknisi sarpras SI/TI
21	Auditor melakukan cek terkait pemisahan fasilitas pengolahan informasi secara fisik yang dikelola oleh organisasi dengan pihak eksternal	Teknisi sarpras SI/TI

Tabel 5.6 Menentukan Resource Setiap Aktifitas pada Control Objective 11.2

No	Aktifitas Audit	Resourece
1	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersedian pencatatan pengunjung yang masuk ke ruang server	Teknisi Sarpras SI/TI
2	Auditor melakukan cek terhadap dokumen pencatatan terkait ketersedian penginformasian tanggal dan waktu maktu masuk pengunjung	Teknisi Sarpras SI/TI
3	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersedian prosedur pengawasan terhadap pengunjung	Teknisi Sarpras SI/TI
4	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur akses masuk ke ruang server	Teknisi Sarpras SI/TI
5	Auditor melakukan cek terhadap dokumen pecatatan pengunjung yang masuk terkait ketersediaan indentitas pengunjung yang masuk	Teknisi Sarpras SI/TI
6	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersesdiaan kontrol akses bagi orang yang memiliki kewenangan untuk masuk	Teknisi Sarpras SI/TI
7	Auditor melakukan cek terhadap kontrol akses yang digunakan terkait penerapan otentikasi 2 faktor	Teknisi Sarpras SI/TI
8	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur pe pengelolaan log akses pengunjung yang berupa buku atau bersifat elektronik	Teknisi Sarpras SI/TI
9	Auditor melakukan cek terhadap penyimpanan log akses yang berupa	Teknisi Sarpras SI/TI

No	Aktifitas Audit	Resourece
	buku atau bersifat elektronik	
10	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur masuk ruang server semua karyawan, kontraktor, pihak external kepada teknis sarpras SI/TI	Teknisi Sarpras SI/TI
11	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan identitas pengenal bagi semua karyawan, kontraktor, dan pihak eksternal yang memiliki akses ke ruang server	Teknisi Sarpras SI/TI
12	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersedian prosedur pelaporan terkait pengunjung yang dikawal dan yang tidak disahkan aksesnya	Teknisi Sarpras SI/TI
13	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersedian prosedur pelaporan terkait pengunjung yang tidak memakai identitas pengenal	Teknisi Sarpras SI/TI
14	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan daftar orang yang memiliki akses ke ruang server	Teknisi Sarpras SI/TI
15	Auditor melakukan cek terhadap daftar orang yang memiliki akses ke ruang server terkait ketersedian hak akses bagi tenaga layanan pendukung dari luar	Teknisi Sarpras SI/TI
16	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur akses masuk bagi tenaga layanan pendukung dari luar	Teknisi Sarpras SI/TI

No	Aktifitas Audit	Resourece
17	Auditor menanyakan terkait ketersediaan prosedur pembaharuan daftar hak askes bagi karyawan atau pihak ketiga yang telah putus kontrak	Teknisi Sarpras SI/TI
18	Auditor menanyakan kepada teknisi sarpras SI/TI ketersediaan daftar hak akses yang diperbaruai dan sebelum diperbarui	Teknisi Sarpras SI/TI

Tabel 5.7 Menentukan Resource Setiap Aktifitas pada Control Objective 11.1.3

No	Aktifitas Audit	Resourece
1	Auditor menanyakan kepada Pengelola administrasi BMN terkait aturan penentuan letak fasilitas seperti pintu dan jendela pada ruang server	Pengelola administrasi BMN
2	Auditor melakukan cek kesesuaian letak pintu dan jendela dengan aturan penentuan letaknya	Teknisi Sarpras SI/TI
3	Auditor melakukan cek terkait adanya tanda keberadaan ruang server	Teknisi Sarpras SI/TI
4	Auditor melakukan cek fasilitas ruang server yang dapat terdengar atau terlihanya informasi atau kegiatan rahasia	Teknisi Sarpras SI/TI
5	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya direktori dan buku telepon interna	Teknisi Sarpras SI/TI
6	Auditor melakukan cek terhadap direktori dan buku telepon internal	Teknisi Sarpras SI/TI

Tabel 5.8 Menentukan Resource Setiap Aktifitas pada Control Objective 11.1.4

No	Aktivitas Audit	Resource
1	Auditor menanyakan kepada Pengelola administrasi BMN terkait ketersediaan pendefinisian saran spesialis tentang memberikan pengamanan ruang server	Pengelola administrasi BMN
2	Auditor melakukan cek terkait ketersediaan penentuan letak dalam dokumen saran spesialis	Pengelola administrasi BMN
3	Auditor melakukan cek terhadap letak ruang server terkait kesesuaian dengan dokumen saran spesialis	Teknisi Sarpras SI/TI
4	Auditor melakukan cek terkait ketersediaan penentuan konstruksi bagunan yang harus digunakan dalam dokumen saran spesialis	Pengelola administrasi BMN
5	Auditor melakukan cek terhadap konstruksi bangunan ruang server terkait kesesuaian dengan dokumen saran spesialis	Teknisi Sarpras SI/TI
6	Auditor melakukan cek terkait ketersediaan penentuan alat pendukung yang harus digunakan dalam dokumen saran spesialis	Pengelola administrasi BMN
7	Auditor melakukan cek terhadap alat pendukung yang ada di ruang server terkait kesesuaian dengan dokumen saran spesialis	Teknisi Sarpras SI/TI

Tabel 5.9 Menentukan Resource Setiap Aktifitas pada Control Objective 11.1.5

No	Aktifitas Audit	Resource
1	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur kerja	Teknisi Sarpras SI/TI
2	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur yang melarang kerja tanpa pengawasan diruang server	Teknisi Sarpras SI/TI
3	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur penguncian ruang server saat ditinggalkan	Teknisi Sarpras SI/TI
4	Auditor melakukan cek terkait adanya pengamanan pada pintu di ruang server	Teknisi Sarpras SI/TI
5	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya peraturan yang melarang kegiatan merekam	Teknisi Sarpras SI/TI

Tabel 5.10 Menentukan Resource Setiap Aktifitas pada Control Objective 11.1.6

No	Aktifitas Audit	Resource
1	Auditor melakukan cek terkait adanya area pengiriman dan penerimaan barang di sekitar ruang server	Teknisi Sarpras SI/TI
2	Auditor menanyakan kepada teknisi sarpras SI/TI terkait pengidentifikasiaan personel yang bertanggung jawab mengawasi di area pengiriman dan penerimaan barang	Teknisi Sarpras SI/TI
3	Auditor menanyakan kepada Pengelola administrasi BMN terkait adanya desing bangunan dan letak area pengiriman dan penerimaan barang	Pengelola administrasi BMN
4	Auditor melakukan cek area pengiriman dan penerimaan barang terkait kesesuaian dengan design yang dibuat	Teknisi Sarpras SI/TI
5	Auditor melakukan cek terhadap area pengiriman dan penerimaan barang terkait keamanan akses ke gedung lain	Teknisi Sarpras SI/TI
6	Auditor menanyakan kepada Pengelola administrasi BMN terkait adanya prosedur pemeriksaan barang	Pengelola administrasi BMN
7	Auditor melakukann cek terkait adanya pencatatan pemeriksaan barang	Teknisi Sarpras SI/TI
8	Auditor menanyakan kepada Pengelola administrasi BMN terkait adanya prosedur manajemen aset	Pengelola administrasi BMN
9	Auditor melakukann cek terkait adanya pencatatan barang yang masuk ke area kerja	Teknisi Sarpras SI/TI

No	Aktifitas Audit	Resource
10	Auditor melakukan cek terkait pemisahan ruang pengiriman dengan ruang penerimaan barang	Teknisi Sarpras SI/TI
11	Auditor melakukan cek terhadap prosedur pemeriksaan barang terkait adanya pemeriksaan barang yang mengalami gangguan	Pengelola administrasi BMN
12	Auditor menanyakan kepada Pengelola administrasi BMN terkait adanya prosedur pelaporan barang yang mengalami gangguan pengiriman	Pengelola administrasi BMN

Tabel 5.11 Menentukan Resource Setiap Aktifitas pada Control Objective 11.2.1

No	Aktifitas Audit	Resource
1	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan ketentuan peletakan peralatan	Teknisi Sarpras SI/TI
2	Auditor melakukan cek terkait kesesuai penempatan peralatan yang ada dengan dokumen ketentuan peletakan peralatan	Teknisi Sarpras SI/TI
3	Auditor melakukan cek terhadap fasilitas pengolahan informasi yang menangangi data sensitif terkait kesesuaian terhadap dokumen ketentuan peletakan	Teknisi Sarpras SI/TI
4	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur pengamanan fasilitas penyimpanan	Teknisi Sarpras SI/TI
5	Auditor melakukan cek terkait keamanan fasilitas penyimpanan	Teknisi Sarpras SI/TI
6	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan daftar peralatan yang membutuhkan pengamanan khusus	Teknisi Sarpras SI/TI
7	Auditor melakukan cek terkait ketersediaan kebutuhan pengamanan yang ada pada daftar peralatan yang membutuhkan pengamanan khusus	Teknisi Sarpras SI/TI
8	Auditor melakukan cek terkait kesesuaian pengamanan yang ada pada peralatan yang membutuhkan pengamanan khusus terhadap kebutuhan yang ditentukan	Teknisi Sarpras SI/TI

No	Aktifitas Audit	Resource
9	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan pengelolaan risiko yang ada diruang server terkait risiko ancaman fisik dan lingkungan	Teknisi Sarpras SI/TI
10	Auditor melakukan cek terkait kesesuaian control yang di adopsi pada dokumen pengelolaan risiko terkait risiko ancaman fisik dan lingkungan	Teknisi Sarpras SI/TI
11	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur mengenai makan, minum dan merokok didekat fasilitas pengolahan informasi	Teknisi Sarpras SI/TI
12	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan ketentuan suhu di ruang server	Teknisi Sarpras SI/TI
13	Auditor melakukan cek kesesuaian suhu dalam ruang server terhadap ketentuuan yang ada	Teknisi Sarpras SI/TI
14	Auditor melakukan cek ketersediaan penangkal petir pada bangunan ruang server	Teknisi Sarpras SI/TI
15	Auditor melakukann cek ketersediaan pelindung elektromagnetik pada peralatan pengolahan informasi rahasia	Teknisi Sarpras SI/TI

Tabel 5.12 Menentukan Resource Setiap Aktifitas pada Control Objective 11.2.2

No	Aktifitas Audit	Resourece
1	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan ketentuan kebutuhan peralatan pendukung di IS-net	Teknisi Sarpras SI/TI
2	Auditor melakukan cek kesesuaian peralatan pendukung yang ada dengan daftar kebutuhan peralatan pendukung	Teknisi Sarpras SI/TI
3	Auditor menanyakan kepada teknis sarpras listrik terkait ketersediaan kebijakan penilaian kapasitas peralatan yang ada terhadap pemenuhan pertumbuhan bisnis dan interaksi dengan peralatan pendukung lainnya	Teknisi Sarpras Listrik
4	Auditor menanyakan kepada teknisi sarpras Listrik terkait ketersediaan penilaian kapasitas peralatan	Teknisi Sarpras SI/TI
5	Auditor menanyakan kepada teknis sarpras listrik terkait adanya pemeriksaan dan pengujian peralatan pendukung untuk memastikan dapat berfungsi dengan baik	Teknisi Sarpras Listrik
6	Auditor melakukan cek terhadap dokumen pemeriksaan dan pengujian peralatan pendukung	Teknisi Sarpras Listrik
7	Auditor melakkukan cek terhadap peralatan pendukung terkait mendeteksi malfungsi	Teknisi Sarpras SI/TI
8	Auditor menanyakan kepada teknisi sarpras listrik terkait ketersediaan kebijakan penggunaan lebih dari 1 sumber setiap peralatan pendukung	Teknisi Sarpras Listrik

Tabel 5.13 Menentukan Resource Setiap Aktifitas pada Control Objective 11.2.3

No	Aktifitas Audit	Resource
1	Auditor melakukan cek pada instalasi kabel listrik dan kabel telekomunikasi terkait penempatan kabel	Teknisi Sarpras SI/TI
2	Auditor melakukan cek terkait adanya perlindungan alternative pada kabel kepada teknis sarpras listrik	Teknisi Sarpras Listrik
3	Auditor melakukan cek terhadap kabel telekomunikasi dan kabel listrik	Teknisi Sarpras SI/TI
4	auditor menyakan kepada teknisi sarpras listrik terkait ketersediaan prosedur instalasi saluran lapis baja	Teknisi Sarpras Listrik
5	Auditor melakukan cek terhadap kabel yang menyambung pada server terkait instalasi saluran lapis baja	Teknisi Sarpras SI/TI
6	Auditor menanyakan kepada teknisi sarpras listrik terkait ketersediaan prosedur penguncian kotak inspeksi dan pemutusan listrik	Teknisi Sarpras Listrik
7	Auditor menanyakan kepada teknisi sarpras listrik terkait ketersediaan prosedur instalasi kabel dengan penggunaan pelindung elektromagnetik	Teknisi Sarpras Listrik
8	Auditor melakukan cek terhadap kabel yang menyambung pada server terkait penggunaan pelindung elektromagnetik	Teknisi Sarpras SI/TI
9	Auditor menayakan kepada teknisi sarpras listrik terkait ketersedian prosedur pengendalian akses ke patch panel dan ruangan kabel	Teknisi Sarpras Listrik

Tabel 5.14 Menentukan Resource Setiap Aktifitas pada Control Objective 11.2.4

No	Aktifitas Audit	Resourece
1	Auditor menayakan kepada Teknisi srarpras SI/TI terkait adanya anjuran pemeliharan peralatan dari pemasok	Teknisi Sarpras SI/TI
2	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait ketersediaan pencatatan pemeliharaan peralatan	Teknisi Sarpras SI/TI
3	Auditor melakukan cek terhadap pencatatan pemeliharaan terkait pemeliharaan peralatan yang dianjurkan oleh pemasok	Teknisi Sarpras SI/TI
4	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait adanya kebijakan asuransi mengenai kebutuhan pemeliharaan peralatan	Teknisi Sarpras SI/TI
5	Auditor melakukan cek terhadap pencatatan pemeliharaan terkait kebutuhan pemeliharaan yang terdapat pada kebijakan asuransi	Teknisi Sarpras SI/TI
6	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait kewenangan proses pemeliharaan peralatan	Teknisi Sarpras SI/TI
7	Auditor melakukan cek terhadap pencatatan pemeliharaan peralatan terkait orang yang berwenang	Teknisi Sarpras SI/TI
8	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait pemeriksaan peralatan setelah dilakukan pemeliharaan	Teknisi Sarpras SI/TI
9	Auditor melakukan cek terhadap pencatatan pemeliharaan peralatan terkait pemeriksaan peralatan setelah dilakukan pemeliharaan	Teknisi Sarpras SI/TI

No	Aktifitas Audit	Resourece
10	Auditor menanyakan kepada Teknisi srarpras SI/TIterkait penjadwalan pemeliharaan peralatan	Teknisi Sarpras SI/TI
11	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait ketersediaan kebijakan proses pemeliharaan yang dilakukan di tempat (ruang server)	Teknisi Sarpras SI/TI
12	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait pemeriksaan peralatan setelah dilakukan pemeliharaan	Teknisi Sarpras SI/TI
13	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait ketersediaan kebijakan pemeliharaan yang akan menggunakan jasa ekternal	Teknisi Sarpras SI/TI
14	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait ketersediaan prosedur penghapusan informasi rahasia pada peralatan yang akan dilakukan pemeliharaan	Teknisi Sarpras SI/TI

Tabel 5.15 Menentukan Resource Setiap Aktifitas pada Control Objective 11.2.5

No	Aktifitas Audit	Resource
1	Auditor menanyakan kepada teknisi sarpras SI/TI terkait pengidentifikasian orang yang memiliki tanggung jawab memberikan izin peminjaman aset	Teknisi Sarpras SI/TI
2	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur peminjaman aset TI	Teknisi Sarpras SI/TI
3	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya pencatatan peminjaman aset	Teknisi Sarpras SI/TI
4	Auditor melakukan cek terkait adanya proses verifikasi batas waktu peminjaman set dalam prosedur pemindahan aset	Teknisi Sarpras SI/TI
5	Auditor melakukan cek pada dokumen pencatatan peminjaman aset terkait adanya pencatatan barang ketika dikembalikan	Teknisi Sarpras SI/TI
6	Auditor melakukan cek pada pencatatan peminjaman aset terkait adanya informasi identitas, jabatan, dan tujuan	Teknisi Sarpras SI/TI

Tabel 5.16 Menentukan Resource Setiap Aktifitas pada Control Objective 11.6.6

NO	Aktifitas Audit	Resource
1	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya kebijakan penggunaan peralatan diluar organisasi	Teknisi Sarpras SI/TI
2	Auditor menanykan kepada teknisi sarpras SI/TI terkait adanya pencatatan penggunaan peralan dan media diluar ruang server	Teknisi Sarpras SI/TI
3	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya instruksi produsen mengenai pengaman peralatan yang dipakai diluar	Teknisi Sarpras SI/TI
4	Auditor menanyakan kepada teknisi sarpras SI/TI terkait pengelolaan risiko terhadap penggunaan peralatan dan media diluar organisasi	Teknisi Sarpras SI/TI
5	Auditor menayakan kepada teknisi sarpras SI/TI terkait adanya prosedur pengalihan barang yang digunakan diluar ruang server	Teknisi Sarpras SI/TI
6	Auditor melakukan cek dokumen pencatatan terkait adanya pendefiniasn nama dan organisasi yang bertanggunng jawab pada peralatan	Teknisi Sarpras SI/TI

Tabel 5.17 Menentukan Resource Setiap Aktifitas pada Control Objective 11.2.7

No	Aktifitas Audit	Resource
1	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersedian prosedur penghapusan informasi pada media penyimpanan	Teknisi Sarpras SI/TI
2	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya proses verifikasi sebelum dibuang atau digunakan kembali terhadap media penyimpanan	Teknisi Sarpras SI/TI
3	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur yang mengatur teknik penghapusan dan penimpaan pada media penyimpanan	Teknisi Sarpras SI/TI
4	Auditor melakukan cek kesesuaian teknik penghapusan atau penimpaan yang digunakan oleh karyawan terhadap prosedur yang ada	Teknisi Sarpras SI/TI

Tabel 5.18 Menentukan Resource Setiap Aktifitas pada Control Objective 11.2.8

No	Aktifitas Audit	Resource
1	Auditor menanyakan terkait ketersediaan prosedur perlindungan perlatan yang tidak diawasi kepada teknis sarpras SI/TI	Teknisi Sarpras SI/TI
2	Auditor melakukan cek terhadap komputer teknis sarpras SI/TI terkait penggunaan password screean saver	Teknisi Sarpras SI/TI
3	Auditor melakukan cek terhadap komputer yang digunakan teknis sarpras SI/TI terkait log-off dari aplikasi atau layanan jaringan ketika tidak digunakan	Teknisi Sarpras SI/TI
4	Auditor melakukan cek terhadap computer atau handphone yang digunakan teknis sarpras SI/TI terkait ketersedian penggunaan password	Teknisi Sarpras SI/TI

Tabel 5.20 Menentukan Resource Setiap Aktifitas pada Control Objective 11.2.9

No	Aktifitas Audit	Resource
1	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur penyimpanan informasi bisnis yang kritis atau sensitive yang berupa dokumen kertas atau media penyimpanan elektronik kepada teknis sarpras SI/TI	Teknisi Sarpras SI/TI
2	Auditor melakukan cek ke dalam ruang server terkait ketersediaan lemeri penyimpanan dokumen yang berisi informasi kritis	Teknisi Sarpras SI/TI
3	Auditor melakukan cek terdahap keamanan lemari penyimpanan dokumen yang berisi informasi kritis	Teknisi Sarpras SI/TI
4	Auditor melakukan cek ke ruang server terkait ketersediaan media penyimpanan elektronik	Teknisi Sarpras SI/TI
5	Auditor menanyakan ketersediaan kepada sarpras SI/TI terkait prosedur penguncian komputer saat digunakaan	Teknisi Sarpras SI/TI
6	Auditor melakukan cek terhadap komputer yang digunakan teknisi sarpras SI/TI diruang server terkait penggunaan password pada komputer	Teknisi Sarpras SI/TI
7	Auditor melakukan cek ketersediaan kepada sarpras SI/TI terkait daftar pengguna peralatan seperti mesin fotokopi, scanner dan kamera digital di ruang server	Teknisi Sarpras SI/TI

No	Aktifitas Audit	Resource
8	Auditor menanyakan kepada sarpras SI/TI terkait ketersediaan peraturan yang melarang penggunaan peralatan seperti mesin fotokopi, scanner dan kamera di ruang server selain daftar pengguna	Teknisi Sarpras SI/TI
9	Auditor melakukan cek ketersediaan kebijakan penghapusan informasi sensitif atau rahasia dari printer	Teknisi Sarpras SI/TI

5.4.3 Mengestimasikan Durasi Setiap Aktifitas Audit

Setelah menentukan aktifitas selanjutnya melakukan estimasi terhadap durasi setiap aktifitas sehingga pada aktifitsa yang ada di proses audit yang akan dilakukan telah dilakukan pertimbangan. Dalam melakukan estimasi durasi waktu diperlukan suatu teknik atau cara yang baik dalam penentuan durasi setiap aktifitasnya sehingga nantinya plan yang dibuat bisa dipertanggung jawabkan.
Perhitungan durasi mengunakan metode estimasi prametric, dimana berdasarkan PMBOK estimasi ini menggunakan hubungan statistic antara data histori dan variable lain untuk menghitung perkiraan pada parameter aktivitas, seperti biaya anggaran dan durasi. Durasi aktifitas dapat ditentukan secara kuantiitaf dengan mengalikan kuantitas pekerjaan yang harus dilakukan oleh jam kerja per unit kerja. Sebagai contoh, sebagai contoh durasi aktifitas pada proyek desain dapat diestimasi dengan mengalikan jumlah gambar dikalikan dengan jumlah jam kerja pergambar atau instalasi kabel per meter dikalikan dengan jumlah jam kerja per meter. Contoh jika sumber daya yang ditugaskan mampu melakukan instalasi 25 meter kabel perjam, durasi yang dibutuhkan untuk mengsinstalasi 1000 meter akan menjadi 40 jam(1000 meter dibagi 25 meter perjam).

Berikut inputan pada penghitungan estimasi ini yaitu :

1. Berdasarkan melihat studi literature pada proses audit di Universitas Airlangga Surabaya yang menyatakan bahwa audit keamanan fisik dan lingkungan di ruang server biasanya dilakukan dalam 2 hari [**7**].
2. Berdasarkan banyaknya aktifitas yang telah diidentifikasi pada proses sebelumnya yaitu sebanyak 144 aktifitas

Proses penghitungan:

- 1 hari kerja = 8 jam, dikarenakan proes audit dlikakukan sebanyak 2 hari maka acauan yang dipakai adalah 16 jam kerja = 960 menit

- Untuk estimasi setiap aktifitasnya adalah 960 menit/144 = 6,6 menit

Pada Tabel 6.17 sampai Tabel 6.31 memaparkan hasil estimasi yang dilakukan untuk setiap aktifitas audit.

Tabel 5.21 Waktu Setiap Aktifitas Pada Control Objective 11.1

No	Aktifitas Audit	Estimasi
1	Auditor menanyakan kepada pengadministrasian BMN terkait adanya kebutuhan perimeter(denah) untuk melindungi aset	6,6 menit
2	Auditor menanyakan kepada Pengadministrasian BMN terkait pendefinisian perimeter keamanan pada ruang server	6,6 menit
3	Auditor melakukan cek ketersediaan letak perimeter dalam dokumen arsitektur bangunan ruang server	6,6 menit
4	Auditor melakukan cek kesesuaian letak bangunan ruang server dengan dokumen arsitektur bangunan	6,6 menit
5	Auditor melakukan cek ketersediaan pendefinisian konstruksi perimeter dalam dokumen arsitektur bangunan ruang server	6,6 menit
6	Auditor melakukan cek kesesuaian konstruksi bangunan dengan dokumen arsitektur bangunan	6,6 menit
7	Auditor melakukan cek terhadap bangunan terkait adanya celah pada bangunan	6,6 menit
8	Auditor melakukan cek pada konstruksi atap, dinding dan lantai	6,6 menit
9	Auditor melakukan cek pada pintu luar ruang server terkait adanya pengamanan akses masuk	6,6 menit
10	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur penguncian pintu dan jendela eksternal ketika ditinggalkan	6,6 menit

No	Aktifitas Audit	Estimasi
11	Auditor melakukan cek terkait adanya area resepsionis	6,6 menit
12	Auditor menanyakan kepada teknisi sarpras SI/TI terkait daftar orang yang boleh masuk keruang server	6,6 menit
13	Auditor melakukan cek terkait adanya batasan fisik dengan ruangan lain	6,6 menit
14	Auditor menanyakan kepada pengadministrasian BMN terkait adanya standar yang yang diacu dalam memilih konstruksi yang anti api	6,6 menit
15	Auditor melakukan cek kesesuaian konsruksi bangunan dengan standar yang diacu	6,6 menit
16	Auditor memeriksa ketersediaan alat pendeteksi penyusup di ruang server	6,6 menit
17	Auditor menanyakan kepada pengadministrasian BMN terkait adanya standar yang yang diacu dalam memilih alat pendeteksi	6,6 menit
18	Auditor menanyakan kepada pengadministrasian BMN terkait adanya daftar spesifikasi alat pendeteksi	6,6 menit
19	Auditor melakukan cek kesesuaian daftar spesifikasi alat pendeteksi penyusup dengan standar yang ada	6,6 menit
20	Auditor melakukan cek ketersediaan ruang komputer	6,6 menit
21	Auditor melakukan cek terkait pemisahan fasilitas pengolahan informasi secara fisik yang dikelola oleh organisasi dengan pihak eksternal	6,6 menit

Tabel 5.22 Waktu Setiap Aktifitas Pada Control Objective 11.1.2

No	Aktifitas Audit	Estimasi
1	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersedian pencatatan pengunjung yang masuk ke ruang server	6,6 menit
2	Auditor melakukan cek terhadap dokumen pencatatan terkait ketersedian penginformasian tanggal dan waktu maktu masuk pengunjung	6,6 menit
3	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersedian prosedur pengawasan terhadap pengunjung	6,6 menit
4	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur akses masuk ke ruang server kepada teknis sarpras SI/TI	6,6 menit
5	Auditor melakukan cek terhadap dokumen pecatatan pengunjung yang masuk terkait ketersediaan indentitas pengunjung yang masuk	6,6 menit
6	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersesdiaan kontrol akses bagi orang yang memiliki kewenangan untuk masuk	6,6 menit
7	Auditor melakukan cek terhadap kontrol akses yang digunakan terkait penerapan otentikasi 2 faktor	6,6 menit
8	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur pe pengelolaan log akses pengunjung yang berupa buku atau bersifat elektronik kepada teknis sarpras SI/TI	6,6 menit
9	Auditor melakukan cek terhadap penyimpanan log akses yang berupa buku atau bersifat elektronik	6,6 menit

No	Aktifitas Audit	Estimasi
10	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur masuk ruang server semua karyawan, kontraktor, pihak external kepada teknis sarpras SI/TI	6,6 menit
11	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan identitas pengenal bagi semua karyawan, kontraktor, dan pihak eksternal yang memiliki akses ke ruang server	6,6 menit
12	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersedian prosedur pelaporan terkait pengunjung yang dikawal dan yang tidak disahkan aksesnya	6,6 menit
13	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersedian prosedur pelaporan terkait pengunjung yang tidak memakai identitas pengenal	6,6 menit
14	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan daftar orang yang memiliki akses ke ruang server kepada teknis sarpras SI/TI	6,6 menit
15	Auditor melakukan cek terhadap daftar orang yang memiliki akses ke ruang server terkait ketersedian hak akses bagi tenaga layanan pendukung dari luar	6,6 menit
16	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur akses masuk bagi tenaga layanan pendukung dari luar	6,6 menit
17	Auditor menanyakan terkait ketersediaan prosedur pembaharuan daftar hak askes bagi karyawan atau pihak ketiga yang telah putus kontrak	6,6 menit

No	Aktifitas Audit	Estimasi
18	Auditor menanyakan kepada teknisi sarpras SI/TI ketersediaan daftar hak akses yang diperbaruai dan sebelum diperbarui	6,6 menit

Tabel 5.24 Waktu Setiap Aktifitas Pada Control Objective 11.1.3

No.	Aktifitas Audit	Estimasi
1	Auditor menanyakan kepada pengadministrasian BMN terkait aturan penentuan letak fasilitas seperti pintu dan jendela pada ruang server	6,6 menit
2	Auditor melakukan cek kesesuaian letak pintu dan jendela dengan aturan penentuan letaknya	6,6 menit
3	Auditor melakukan cek terkait adanya tanda keberadaan ruang server	6,6 menit
4	Auditor melakukan cek fasilitas ruang server yang dapat terdengar atau terlihanya informasi atau kegiatan rahasia	6,6 menit
5	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya direktori dan buku telepon internal	6,6 menit
6	Auditor melakukan cek terhadap pengamanan direktori dan buku telepon internal	6,6 menit

Tabel 5.25 Waktu Setiap Aktifitas Pada Control Objective 11.1.4

No	Aktivitas Audit	Estimasi
1	Auditor menanyakan kepada pengadministrasian BMN terkait ketersediaan pendefinisian saran spesialis tentang memberikan pengamanan ruang server	6,6 menit
2	Auditor melakukan cek terkait ketersediaan penentuan letak dalam dokumen saran spesialis	6,6 menit

No	Aktivitas Audit	Estimasi
3	Auditor melakukan cek terhadap letak ruang server terkait kesesuaian dengan dokumen saran spesialis	6,6 menit
4	Auditor melakukan cek terkait ketersediaan penentuan konstruksi bagunan yang harus digunakan dalam dokumen saran spesialis	6,6 menit
5	Auditor melakukan cek terhadap konstruksi bangunan ruang server terkait kesesuaian dengan dokumen saran spesialis	6,6 menit
6	Auditor melakukan cek terkait ketersediaan penentuan alat pendukung yang harus digunakan dalam dokumen saran spesialis	6,6 menit
7	Aduditor menanyakan kepada teknisi sarpras listrik terkait ketersedian pendefinisian spesifikasi alat pendukung yang ada	6,6 menit
8	Auditor melakukan cek terhadap alat pendukung yang ada di ruang server terkait kesesuaian dengan dokumen saran spesialis	6,6 menit

Tabel 5.26 Waktu Setiap Aktifitas Pada Control Objective 11.1.5

No	Aktifitas Audit	Estimasi
1	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur kerja	6,6 menit
2	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur yang melarang kerja tanpa pengawasan diruang server	6,6 menit
3	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur penguncian ruang server saat ditinggalkan	6,6 menit

4	Auditor melakukan cek terkait adanya pengamanan pada pintu di ruang server	6,6 menit
5	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya peraturan yang melarang kegiatan merekam	6,6 menit

Tabel 5.27 Waktu Setiap Aktifitas Pada Control Objective 11.1.6

No	Aktifitas Audit	Estimasi
1	Auditor melakukan cek terkait adanya area pengiriman dan penerimaan barang di sekitar ruang server	6,6 menit
2	Auditor menanyakan kepada teknisi sarpras SI/TI terkait pengidentifikasiaan personel yang bertanggung jawab mengawasi di area pengiriman dan penerimaan barang	6,6 menit
3	Auditor menanyakan kepada pengadministrasian BMN terkait adanya desing bangunan dan letak area pengiriman dan penerimaan barang	6,6 menit
4	Auditor melakukan cek area pengiriman dan penerimaan barang terkait kesesuaian dengan design yang dibuat	6,6 menit
5	Auditor melakukan cek terhadap area pengiriman dan penerimaan barang terkait keamanan akses ke gedung lain	6,6 menit
6	Auditor menanyakan kepada pengadministrasian BMN terkait adanya prosedur pemeriksaan barang	6,6 menit
7	Auditor melakukann cek terkait adanya pencatatan pemeriksaan barang	6,6 menit
8	Auditor menanyakan kepada pengadministrasian BMN terkait adanya prosedur manajemen aset	6,6 menit
9	Auditor melakukann cek terkait adanya pencatatan barang yang masuk ke area kerja	6,6 menit

No	Aktifitas Audit	Estimasi
10	Auditor melakukan cek terkait pemisahan ruang pengiriman dengan ruang penerimaan barang	6,6 menit
11	Auditor melakukan cek terhadap prosedur pemeriksaan barang terkait adanya pemeriksaan barang yang mengalami gangguan	6,6 menit
12	Auditor menanyakan kepada pengadministrasian BMN terkait adanya prosedur pelaporan barang yang mengalami gangguan pengiriman	6,6 menit

Tabel 5.28 Waktu Setiap Aktifitas Pada Control Objective 11.2.1

No	Aktifitas Audit	Estimasi
1	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan ketentuan peletakan peralatan	6,6 menit
2	Auditor melakukan cek terkait kesesuai penempatan peralatan yang ada dengan dokumen ketentuan peletakan peralatan	6,6 menit
3	Auditor melakukan cek terhadap fasilitas pengolahan informasi yang menangangi data sensitif terkait kesesuaian terhadap dokumen ketentuan peletakan	6,6 menit
4	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur pengamanan fasilitas penyimpanan	6,6 menit
5	Auditor melakukan cek terkait keamanan fasilitas penyimpanan	6,6 menit
6	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan daftar peralatan yang membutuhkan pengamanan khusus	6,6 menit

No	Aktifitas Audit	Estimasi
7	Auditor melakukan cek terkait ketersediaan kebutuhan pengamanan yang ada pada daftar peralatan yang membutuhkan pengamanan khusus	6,6 menit
8	Auditor melakukan cek terkait kesesuaian pengamanan yang ada pada peralatan yang membutuhkan pengamanan khusus terhadap kebutuhan yang ditentukan	6,6 menit
9	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan pengelolaan risiko yang ada diruang server terkait risiko ancaman fisik dan lingkungan	6,6 menit
10	Auditor melakukan cek terkait kesesuaian control yang di adopsi pada dokumen pengelolaan risiko terkait risiko ancaman fisik dan lingkungan	6,6 menit
11	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur mengenai makan, minum dan merokok didekat fasilitas pengolahan informasi	6,6 menit
12	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan ketentuan suhu di ruang server	6,6 menit
13	Auditor melakukan cek kesesuaian suhu dalam ruang server terhadap ketentuuan yang ada	6,6 menit
14	Auditor melakukan cek ketersediaan penangkal petir pada bangunan ruang server	6,6 menit
15	Auditor melakukann cek ketersediaan pelindung elektromagnetik pada peralatan pengolahan informasi rahasia	6,6 menit

Tabel 5.29 Waktu Setiap Aktifitas Pada Control Objective 11.2.2

No	Aktifitas Audit	Estimasi
1	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan ketentuan kebutuhan peralatan pendukung di IS-net	6,6 menit
2	Auditor melakukan cek kesesuaian peralatan pendukung yang ada dengan daftar kebutuhan peralatan pendukung	6,6 menit
3	Auditor menanyakan kepada teknis sarpras listrik terkait ketersediaan kebijakan penilaian kapasitas peralatan yang ada terhadap pemenuhan pertumbuhan bisnis dan interaksi dengan peralatan pendukung lainnya	6,6 menit
4	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan penilaian kapasitas peralatan	6,6 menit
5	Auditor menanyakan kepada teknis sarpras listrik terkait adanya pemeriksaan dan pengujian peralatan pendukung untuk memastikan dapat berfungsi dengan baik	6,6 menit
6	Auditor melakukan cek terhadap dokumen pemeriksaan dan pengujian peralatan pendukung	6,6 menit
7	Auditor melakkukan cek terhadap peralatan pendukung terkait mendeteksi malfungsi	6,6 menit
8	Auditor menanyakan kepada teknisi sarpras listrik terkait ketersediaan kebijakan penggunaan lebih dari 1 sumber setiap peralatan pendukung	6,6 menit

Tabel 5.30 Waktu Setiap Aktifitas Pada Control Objective 11.2.3

No	Aktifitas Audit	Estimasi
1	Auditor melakukan cek pada instalasi kabel listrik dan kabel telekomunikasi terkait penempatan kabel	6,6 menit
2	Auditor melakukan cek terkait adanya perlindungan alternative pada kabel kepada teknis sarpras listrik	6,6 menit
3	Auditor melakukan cek terhadap kabel telekomunikasi dan kabel listrik	6,6 menit
4	auditor menyakan kepada teknisi sarpras listrik terkait ketersediaan prosedur instalasi saluran lapis baja	6,6 menit
5	Auditor melakukan cek terhadap kabel yang menyambung pada server terkait instalasi saluran lapis baja	6,6 menit
6	Auditor menanyakan kepada teknisi sarpras listrik terkait ketersediaan prosedur penguncian kotak inspeksi dan pemutusan listrik	6,6 menit
7	Auditor menanyakan kepada teknisi sarpras listrik terkait ketersediaan prosedur instalasi kabel dengan penggunaan pelindung elektromagnetik	6,6 menit
8	Auditor melakukan cek terhadap kabel yang menyambung pada server terkait penggunaan pelindung elektromagnetik	6,6 menit
9	Auditor menayakan kepada teknisi sarpras listrik terkait ketersedian prosedur pengendalian akses ke patch panel dan ruangan kabel	6,6 menit

Tabel 5.31 Waktu Setiap Aktifitas Pada Control Objective 11.2.4

No	Aktifitas Audit	Estimasi
1	Auditor menayakan kepada Teknisi srarpras SI/TI terkait adanya anjuran pemeliharan peralatan dari pemasok	6,6 menit
2	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait ketersediaan pencatatan pemeliharaan peralatan	6,6 menit
3	Auditor melakukan cek terhadap pencatatan pemeliharaan terkait pemeliharaan peralatan yang dianjurkan oleh pemasok	6,6 menit
4	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait adanya kebijakan asuransi mengenai kebutuhan pemeliharaan peralatan	6,6 menit
5	Auditor melakukan cek terhadap pencatatan pemeliharaan terkait kebutuhan pemeliharaan yang terdapat pada kebijakan asuransi	6,6 menit
6	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait kewenangan proses pemeliharaan peralatan	6,6 menit
7	Auditor melakukan cek terhadap pencatatan pemeliharaan peralatan terkait orang yang berwenang	6,6 menit
8	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait ananya pemeriksaan peralatan setelah dilakukan pemeliharaan	6,6 menit
9	Auditor melakukan cek terhadap pencatatan pemeliharaan peralatan terkait pemeriksaan peralatan setelah dilakukan pemeliharaan	6,6 menit
10	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait adanya penjadwalan pemeliharaan peralatan	6,6 menit
11	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait ketersediaan kebijakan proses	6,6 menit

No	Aktifitas Audit	Estimasi
	pemeliharaan yang dilakukan di tempat (ruang server)	
12	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait pemeriksaan peralatan setelah dilakukan pemeliharaan	6,6 menit
13	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait ketersediaan kebijakan pemeliharaan yang akan menggunakan jasa ekternal	6,6 menit
14	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait ketersediaan prosedur penghapusan informasi rahasia pada peralatan yang akan dilakukan pemeliharaan	6,6 menit

Tabel 5.32 Waktu Setiap Aktifitas Pada Control Objective 11.2.5

No	Aktifitas Audit	Estimasi
1	Auditor menanyakan kepada teknisi sarpras SI/TI terkait pengidentifikasian orang yang memiliki tanggung jawab memberikan izin peminjaman aset	6,6 menit
2	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur peminjaman aset TI	6,6 menit
3	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya pencatatan peminjaman aset	6,6 menit
4	Auditor melakukan cek terkait adanya proses verifikasi batas waktu peminjaman set dalam prosedur pemindahan aset	6,6 menit
5	Auditor melakukan cek pada dokumen pencatatan peminjaman aset terkait adanya pencatatan barang ketika dikembalikan	6,6 menit
6	Auditor melakukan cek pada pencatatan peminjaman aset terkait adanya informasi	6,6 menit

No	Aktifitas Audit	Estimasi
	identitas, jabatan, dan tujuan	

Tabel 5.33 Waktu Setiap Aktifitas Pada Control Objective 11.2.6

NO	Aktifitas Audit	Estimasi
1	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya kebijakan penggunaan peralatan diluar organisasi	6,6 menit
2	Auditor menanykan kepada teknisi sarpras SI/TI terkait adanya pencatatan penggunaan peralan dan media diluar ruang server	6,6 menit
3	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya instruksi produsen mengenai pengaman peralatan yang dipakai diluar	6,6 menit
4	Auditor menanyakan kepada teknisi sarpras SI/TI terkait pengelolaan risiko terhadap penggunaan peralatan dan media diluar organisasi	6,6 menit
5	Auditor menayakan kepada teknisi sarpras SI/TI terkait adanya prosedur pengalihan barang yang digunakan diluar ruang server	6,6 menit
6	Auditor melakukan cek dokumen pencatatan terkait adanya pendefiniasn nama dan organisasi yang bertanggunng jawab pada peralatan	6,6 menit

Tabel 5.34 Waktu Setiap Aktifitas Pada Control Objective 11.2.7

No	Aktifitas Audit	Estimasi
1	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersedian prosedur penghapusan informasi pada media penyimpanan	6,6 menit
2	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya proses verifikasi sebelum dibuang atau digunakan kembali terhadap media penyimpanan	6,6 menit
3	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur yang mengatur teknik penghapusan dan penimpaan pada media penyimpanan	6,6 menit
4	Auditor melakukan cek kesesuaian teknik penghapusan atau penimpaan yang digunakan oleh karyawan terhadap prosedur yang ada	6,6 menit

Tabel 5.35 Waktu Setiap Aktifitas Pada Control Objective 11.2.8

No	Aktifitas Audit	Estimasi
1	Auditor menanyakan terkait ketersediaan prosedur perlindungan perlatan yang tidak diawasi kepada teknis sarpras SI/TI	6,6 menit
2	Auditor melakukan cek terhadap komputer teknis sarpras SI/TI terkait penggunaan password screean saver	6,6 menit
3	Auditor melakukan cek terhadap komputer yang digunakan teknis sarpras SI/TI terkait log-off dari aplikasi atau layanan jaringan ketika tidak digunakan	6,6 menit
4	Auditor melakukan cek terhadap computer dan handphone yang digunakan teknis sarpras SI/TI terkait ketersedian penggunaan password	6,6 menit

Tabel 5.36 Waktu Setiap Aktifitas Pada Control Objective 11.2.9

No	Aktifitas Audit	Estimasi
1	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur penyimpanan informasi bisnis yang kritis atau sensitive yang berupa dokumen kertas atau media penyimpanan elektronik kepada teknis sarpras SI/TI	6,6 menit
2	Auditor melakukan cek ke dalam ruang server terkait ketersediaan lemeri penyimpanan dokumen yang berisi informasi kritis	6,6 menit
3	Auditor melakukan cek terdahap ketersedian pengaman lemari penyimpanan dokumen yang berisi informasi kritis	6,6 menit
4	Auditor melakukan cek ke ruang server terkait ketersediaan media penyimpanan elektronik	6,6 menit
5	Auditor menanyakan ketersediaan kepada sarpras SI/TI terkait prosedur penguncian komputer saat digunakaan	6,6 menit
6	Auditor melakukan cek terhadap komputer yang digunakan teknisi sarpras SI/TI diruang server terkait penggunaan password pada computer	6,6 menit
7	Auditor melakukan cek ketersediaan kepada sarpras SI/TI terkait daftar pengguna peralatan seperti mesin fotokopi, scanner dan kamera digital di ruang server	6,6 menit
8	Auditor menanyakan kepada sarpras SI/TI terkait ketersediaan peraturan yang melarang penggunaan peralatan seperti mesin fotokopi, scanner dan kamera di ruang server selain daftar pengguna	6,6 menit
9	Auditor melakukan cek ketersediaan kebijakan penghapusan informasi sensitif atau rahasia dari printer	6,6 menit

5.4.4 Mengurutkan Aktifitas Audit

Predecessor merupakan komponen yang menjadi acuan dari permulaan suatu aktifitas. Predecessor menunjukkan nomor komponen aktivitas mana yang harus selesai sebelum aktivitas ini dimulai. Nomor WBS penentu komponen aktifitas mana yang harus selesai. Sebelum menentukan predecessorsnya makan diperlukan untuk mengurutkan aktifitas terlebih dahulu. Dalam mengurutkan aktifiitas audit didasarkan dari pengelompokan resource yang bertanggung jawab sehingga nantinya dapat mengefisiensikan waktu saat melakukan audit Gambar berikut Menjelaskan contoh penggunaan predecessor pada aktifitas audit

No. WBS	Aktifitas Audit	Durasi	Start	Finish	Predecessors	Resource Name
1.	Auditor menanyakan kepada pengadministrasian BMN terkait adanya kebutuhan perimeter(Denah) untuk melindungi aset	6,6 mins	Tue 02/01/18	Tue 02/01/18		Pengelola Administrasi BMN
2.	Auditor menanyakan kepada Pengadministrasian BMN terkait pendefinisian perimeter(Denah) keamanan pada ruang server	6,6 mins	Tue 02/01/18	Tue 02/01/18	1	Pengelola Administrasi BMN
3.	Auditor melakukan cek ketersediaan letak perimeter dalam denah bangunan ruang server	6,6 mins	Tue 02/01/18	Tue 02/01/18	2	Pengelola Administrasi BMN
4.	Auditor melakukan cek ketersediaan pendefinisian konstruksi perimeter dalam denah bangunan ruang server	6,6 mins	Tue 02/01/18	Tue 02/01/18	3	Pengelola Administrasi BMN
5.	Auditor menanyakan kepada pengadministrasian BMN terkait adanya standar yang yang diacu dalam memilih konstruksi yang anti api	6,6 mins	Tue 02/01/18	Tue 02/01/18	4	Pengelola Administrasi BMN
6.	Auditor menanyakan kepada pengadministrasian BMN terkait adanya standar yang yang diacu dalam memilih alat pendeteksi	6,6 mins	Tue 02/01/18	Tue 02/01/18	5	Pengelola Administrasi BMN
7.	Auditor menanyakan kepada pengadministrasian BMN terkait adanya daftar spesifikasi alat pendeteksi	6,6 mins	Tue 02/01/18	Tue 02/01/18	6	Pengelola Administrasi BMN
8.	Auditor menanyakan kepada pengadministrasian BMN terkait aturan penentuan letak fasilitas seperti pintu dan jendela pada ruang server	6,6 mins	Tue 02/01/18	Tue 02/01/18	7	Pengelola Administrasi BMN
9.	Auditor menanyakan kepada pengadministrasian BMN terkait ketersediaan pendefinisian saran spesialis tentang memberikan pengamanan ruang server	6,6 mins	Tue 02/01/18	Tue 02/01/18	8	Pengelola Administrasi BMN
10.	Auditor melakukan cek terkait ketersediaan penentuan letak dalam dokumen saran spesialis	6,6 mins	Tue 02/01/18	Tue 02/01/18	9	Pengelola Administrasi BMN

Gambar 5.2 Pengurutan aktifitas audit

5.5 Pembuatan audit Program

Dalam penyusunan dokumen *audit program* pada IS-NET berdasarkan ISO/IEC 27002:2013 klausul 11, dalam hal ini penulis melakukan pengambangan dari dokumen audit program sebelumnya milik Stephen Crishtian [**7**] dan Yudhis Cahyo Eko [**3**]. Sebelum audit program dibuat maka diperlukan untuk membuat daftar cek audit

5.5.1 Membuat daftar Cek

Setelah aktifitas audit teridentifikasi, maka langkah selanjutnya adalah membuat daftar cek audit yang berupa pertanyaan-pertanyaan untuk memastikan adanya temuan audit. dalam pembuatan daftar cek audit dilakukan dengan cara mengacu pada aktifitas audit yang berdasarkan implementation guidance pada setiap *control objective.* pada Tabel berikut ini menjelaskan cara pembuatan daftar cek audit dengan mencontohkan *control objective physical security perimeter*:

Tabel 5.8 Contoh Pembuatan Daftar Cek Audit

PERANGKAT AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI DI RUANG SERVER JURUSAN SISTEM INFORMASI ITS (IS-NET)							
Auditor:			*1. Secure Areas*				
			1.1 Physical Security Perimeter				
Tanggal Audit :			Kontrol : Perimeter keamanan (batasan seperti dinding, pintu masuk yang dikendalikan dengan kartu atau meja resepsionis yang dijaga) harus digunakan untuk melindungi area yang berisi informasi dan fasilitas pengolahan informasi.				
dd	mm	yy					
No.	**Aktifitas Audit**	**Daftar Cek Audit**	**Test**	**Iya**	**Tidak**	**Partial**	**Bukti**
P 11.1.a	Auditor menanyakan kepada pengadministrasian BMN terkait adanya kebutuhan perimeter untuk melindungi aset	Apakah terdapat pengidentifikasian kebutuhan perimeter untuk pengamanan aset?	Compliance				(dokumen kebutuhan perimeter keamanan aset)
		Temuan:					
	Auditor menanyakan kepada Pengadministrasian BMN terkait pendefinisian perimeter keamanan pada ruang server	Apakah terdapat pendefinisian perimeter keamanan pada ruang server?	Substantive				(desain arsitektur bangunan ruang server)
		Temuan:					
	Auditor melakukan cek ketersediaan letak perimeter dalam dokumen arsitektur bangunan ruang server	Apakah dalam desain arsitektur bangunan terdapat pendefinisian letak perimeter?	Substantive				(desain arsitektur bangunan ruang server)
		Temuan					

	Auditor melakukan cek kesesuaian letak bangunan ruang server dengan dokumen arsitektur bangunan	apakah letak bangunan ruang server sesuai dengan desain arsitektur?	Compliance				(checklist kesesuaian letak bangunanan)
		Temuan:					
	Auditor melakukan cek ketersediaan pendefinisian konstruksi perimeter dalam dokumen arsitektur bangunan ruang server	Apakah terdapat pendefinisian konstruksi perimeter pada desain arsitektur bangunan ruang server?	Substantive				(desain arsitektur bangunan ruang server)
		Temuan:					
	Auditor melakukan cek kesesuaian konstruksi bangunan dengan dokumen arsitektur bangunan	Apakah konstruksi bangunan ruang server sesuai dengan desain arsitektur?	Substantive				(checklist keseuaian)
		Temuan:					
P 11.1.b	Auditor melakukan cek terhadap bangunan terkait adanya celah pada bangunan terkait kedap suara	Apakah terdapat celah pada bangunan diruang server sehingga aktifitas di dalam dapat terdengar?	Substantive				(foto celah bangunan)
		Temuan:					
	Auditor melakukan cek pada konstruksi atap, dinding dan lantai	Apakah atap dinding dan lantai terbuat dari konstruksi yang kuat (beton)? (periksa kekuatan atap dinding dengan melihat dan memegang)	Compliance				(foto atap, dinding, dan lantai)
		Temuan:					
	Auditor melakukan cek pada pintu luar ruang	Apakah terdapat kunci atau gembok pada pintu luar ruang server atau alat pengaman	Substantive				(foto kunci atau gembok atau alau pengaman lainnya)

	server terkait adanya pengamanan akses masuk	lainnya?					
		Temuan:					
	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur penguncian pintu dan jendela eksternal ketika ditinggalkan	Apakah terdapat prosedur penguncian pintu atau jendela eksternal ketika ditinggalkan?	Compliance				(prosedur penguncian pintu dan jendela)
		Temuan:					
P 11.1.c	Auditor melakukan cek terkait adanya area resepsionis	Apakah terdapat ruang resepsionis di area ruang server?	Compliance				(foto ruang resepsionis)
		Temuan:					
	Auditor menanyakan kepada teknisi sarpras SI/TI terkait daftar orang yang boleh masuk keruang server	Apakah terdapat daftar orang yang boleh masuk ke ruang server?	Substantive				(dafatar orang yang boleh masuk ruang server)
		Temuan:					
P 11.1.d	Auditor melakukan cek terkait adanya batasan fisik dengan ruangan lain	Apakah terdapat batasan fisik antara ruang server dengan ruangan lain?	Substantive				(batasan fisik ruang server)
		Temuan:					

P 11.1.e	Auditor menanyakan kepada pengadministrasian BMN terkait adanya standar yang yang diacu dalam memilih konstruksi yang anti api	Apakah mempunyai standar yang diacu untuk memilih konstruksi bangunan yang anti api?	Compliance				(standar regulasi kebakaran)
		Temuan:					
	Auditor melakukan cek kesesuaian konsruksi bangunan dengan standar yang diacu	Apakah konstruksi bangunan sesuai dengan standar yang diacu?	Substantive				(checklist kesesuaian bangun anti api)
		Temuan:					
P 11.1.f	Auditor memeriksa ketersediaan alat pendeteksi penyusup di ruang server	Apakah terdapat alat pendeteksi penyusup di ruang server?	Substantive				(foto alat pendeteksi penyusup)
		Temuan:					
	Auditor menanyakan kepada pengadministrasian BMN terkait adanya standar yang yang diacu dalam memilih alat pendeteksi	Apakah terdapat standar yang diacu dalam pemilihan alat pendeteksi penyusup?	Compliance				(standar pemilihan alat pendeteksi)
		Temuan:					
	Auditor melakukan cek kesesuaian alat pendeteksi penyusup dengan standar yang ada	Apakah alat pendeteksi yang ada telah sesuai dengan standar yang diacu?	Compliance				(checklist kesesuaian alat pendeteksi)
		Temuan:					
	Auditor melakukan cek ketersediaan ruang	Apakah di dalam ruang server terdapat sekat untuk ruang computer?	Substantive				(sekat ruang komputer)

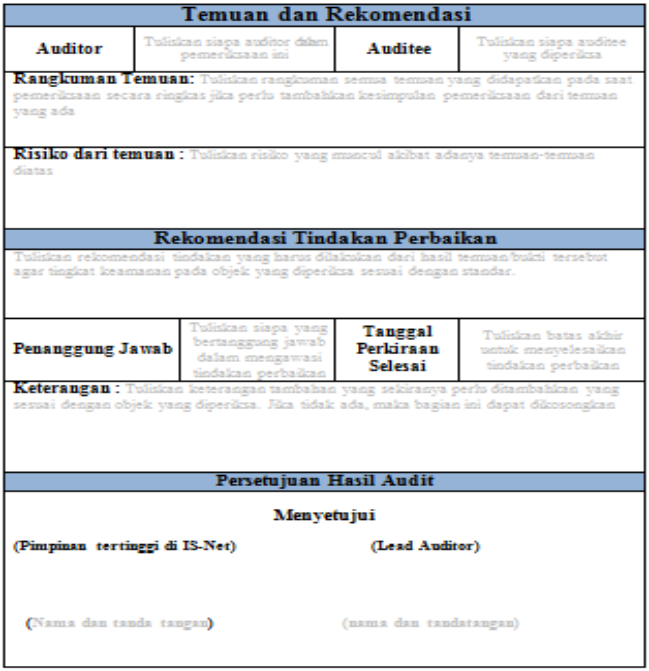
	komputer	Temuan:					
P 11.1.g	Auditor melakukan cek terkait pemisahan fasilitas pengolahan informasi secara fisik yang dikelola oleh organisasi dengan pihak eksternal	Apakah fasilitas pengolahan informasi yang dikelola oleh organisasi teal dipisahkan dengan yang dikelola pihak eksternal?	Compliance				(foto pemisah fasilitas pengolahan informasi)
		Temuan:					

5.5.2 Pembuatan Template Temuan dan Rekomendasi

Dalam pembuatan template ini dihasilkan dari melihat dan mengkaji studi literature sehingga dapat menghasilkan sebuah template yang dapat mempresentasikan

Template temuan dan rekomendasi audit dibuat untuk dapat memudahkan auditor untuk merangkum semua temuan yang ada, membuat rekomendasinya, hingga menyetujui hasil audit yang dibuat. Menurut ISO 19011:2011, dalam dokumen kerja audit minimal harus ada formulir yang merekam informasi seperti bukti pendukung, temuan audit dan rekaman rapat. Pada laporan audit juga perlu disertakan antara lain auditor, pihak yang diaudit atau auditee, temuan audit, dan rencana aksi *follow-up* yang disetujui. Sehingga pada *template* temuan dan rekomendasi, disertakan kolom "Auditor" untuk menuliskan siapa orang yang bertugas melaksanakan auditor, sedangkan kolom "Auditee" untuk menuliskan unit mana yang sedang diaudit. Kemudian kolom "Rangkuman Temuan" disertakan untuk memudahkan auditor untuk menuliskan fakta-fakta temuan yang didapat selama melaksanakan audit. Fakta-fakta temuan tersebut pasti memiliki risiko apabila tidak segera ditindaklanjuti, maka dari itu disertakan pula kolom "Risiko dari Temuan" untuk memastikan auditor juga menuliskan risiko dari fakta-fakta temuan sehingga akan lebih terlihat tingkat kepentingan melakukan tindakan perbaikan. Selanjutnya kolom "Rekomendasi tindakan perbaikan" disertakan untuk memastikan auditor juga menentukan tindakan perbaikan atau aksi *follow-up* apa yang harus dilakukan untuk temuan yang didapat. Agar pelaksanaan tindakan perbaikan jelas, maka disertakan kolom "Penanggung jawab" yang disediakan untuk menuliskan siapa yang bertanggung jawab melaksanakan dan mengawasi pelaksanaan tindakan perbaikan serta kolom "Tanggal Perkiraaan Selesai" untuk menuliskan *deadline* pengerjaan tindakan perbaikan sehingga jelas kapan tindakan perbaikan harus diselesaikan.

Terdapat kolom "Keterangan" yang disediakan untuk menuliskan hal-hal lain selain yang ada pada komponen-komponen sebelumnya. Dan terakhir, terdapat kolom "Persetujuan Hasil Audit" yang disertakan karena hasil audit yang dilakukan membutuhkan verifikasi dari pihak auditee. Pada Gambar 5.2 berikut ini adalah template atau formulir temuan dan rekomen dasi audit:



Temuan dan Rekomendasi

Auditor	Tuliskan siapa auditor dalam pemeriksaan ini	**Auditee**	Tuliskan siapa auditee yang diperiksa

Rangkuman Temuan: Tulisikan rangkuman semua temuan yang didapatkan pada saat pemeriksaan secara ringkas jika perlu tambahkan kesimpulan pemeriksaan dari temuan yang ada

Risiko dari temuan : Tulisikan risiko yang muncul akibat adanya temuan-temuan diatas

Rekomendasi Tindakan Perbaikan

Tulisikan rekomendasi tindakan yang harus dilakukan dari hasil temuan/bukti tersebut agar tingkat keamanan pada objek yang diperiksa sesuai dengan standar.

Penanggung Jawab	Tulisikan siapa yang bertanggung jawab dalam mengawasi tindakan perbaikan	**Tanggal Perkiraan Selesai**	Tulisikan batas akhir untuk menyelesaikan tindakan perbaikan

Keterangan : Tulisikan keterangan tambahan yang sekiranya perlu ditambahkan yang sesuai dengan objek yang diperiksa. Jika tidak ada, maka bagian ini dapat dikosongkan

Persetujuan Hasil Audit

Menyetujui

(Pimpinan tertinggi di IS-Net)	**(Lead Auditor)**
(Nama dan tanda tangan)	(nama dan tandatangan)

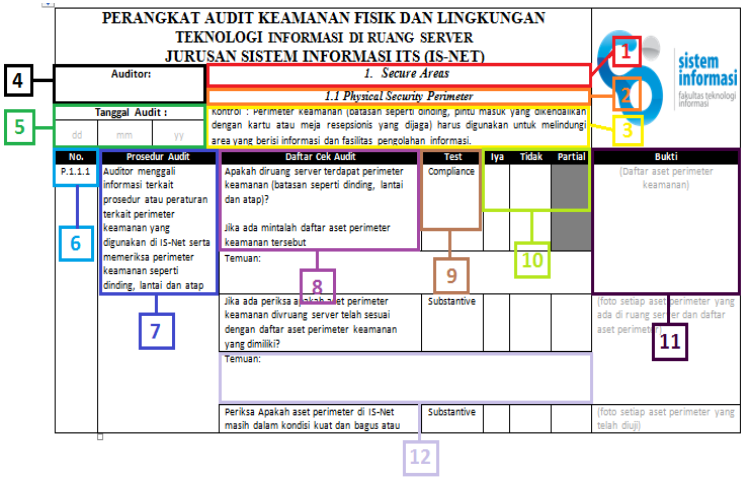
Gambar 5.3 Template Temuan dan Rekomendasi

5.6 Pembuatan Panduan Penggunaan Audit Program

Panduan penggunaan *audit program* disusun untuk memudahkan pengguna perangkat audit dalam memahami cara penggunaan *audit program* yang telah disusun, sehingga diharapkan perangkat audit yang telah dibuat dapat digunakan dengan baik dan benar.
Berikut adalah bagian-bagian yang akan dibahas pada panduan penggunaan *audit program*:

1. **Penjelasan komponen penyusun audit program**

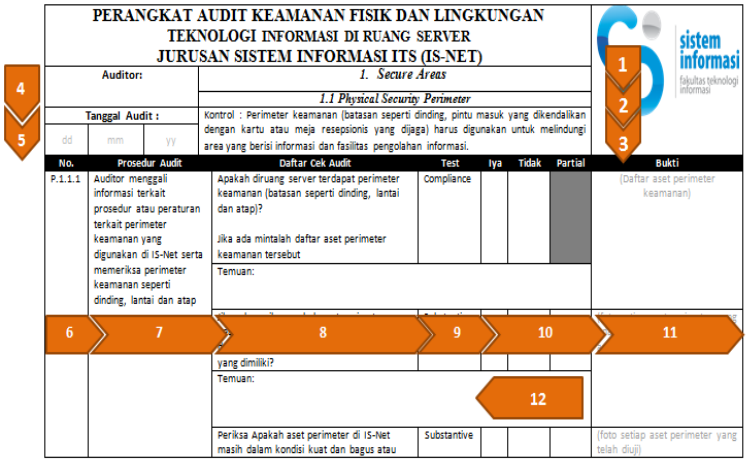
   Pada bagian ini dijelaskan semua komponen penyusun audit program, dari sub klausul, kontrol, penjelasan control, nomor prosedur, prosedur audit, daftar cek audit, opsi jawaban, hingga penyusun tabel temuan dan rekomendasi. Pada Gambar berikut ini adalah contoh komponen-komponen (yang diberi penomoran) yang dijelaskan pada bagian ini :



Gambar 5.4 Komponen Penyusun Audit program

2. **Langkah-langkah penggunaan audit program**

Setelah diberikan penjelasan cara mengisi tiap komponen penyusun audit program yang ada, pada bagian ini akan dijelaskan bagaimana langkah-langkah menggunakan audit program. Pada Gambar berikut ini adalah salah satu contoh gambar urutan langkah pengisian prosedur dan daftar cek audit. Secara keseluruhan penjelasannya terdapat pada dokumen *audit program*.



Gambar 5.5 Langkah-langkah Penggunaan Audit program

3. Contoh Pengisian audit program

Setelah dijelaskan mengenai langkah demi langkah menggunakan audit program, pada bagian ini akan dijelaskan contoh mengisi atau menggunakan masing-masing komponen penyusun audit program yang telah dibuat agar auditor lebih memahami bagaimana cara menggunakan audit program. Pada Gambar berikut ini adalah salah satu contoh gambar penggunaan prosedur dan daftar cek audit pada kontrol 11.2.3. untuk melihat semua contoh pengisian dapat dilihat dalam lampiran D

PERANGKAT AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI DI RUANG SERVER JURUSAN SISTEM INFORMASI ITS (IS-NET)

Auditor:	*2. Equipment Security*
	2.3 Cabling Security
Tanggal Audit : dd mm yy	Kontrol : Kabel listrik dan telekomunikasi yang membawa data atau mendukung layanan informasi pendukung harus dilindungi dari intersepsi atau kerusakan.

No.	Prosedur Audit	Daftar Cek Audit	Test	Iya	Tidak	Partial	Bukti
P.2.3.1	Auditor memeriksa instalasi kabel listrik dan kabel telekomunikasi	a. Apakah terdapat dokumen prosedur terkait instalasi kabel di ruang server?	Compliance	✓			*Tersedia dokumen prosedur instalasi kabel*
		Temuan:					
		b. Periksa apakah semua kabel listrik dan kabel telekomunikasi telah berada di bawah lantai?	Substantive	✓			*Semua kabel listrik dan kabel telekomunikasi berada dibawah lantai* (Foto Kabel listrik dan kabel telekomunikasi yang berada dibawah lantai)
		Temuan:					
		c. Periksa apakah instalasi kabel listrik dan kabel telekomunikasi telah dipisahkan untuk mencegah terjadinya gangguan?	Substantive		✓		*Kabel listrik dan kabel telekomunikasi tidak dipisahkan* (Foto Kabel listrik dan kabel telekomunikasi)
		Temuan: *pada saat penginstalasian kabel, kabel listrik dan kabel telekomunikasi tidak dipisahkan*					
P.2.3.2	Auditor memeriksa perlindungan instalasi saluran kabel daya dan	a. Periksa apakah kabel listrik dan kabel telekomunikasi telah dilindungi dengan pelapis baja?	Substantive			✓	*Hanya sebagian kabel yang dilindungi pelapis*

Gambar 5.6 Contoh Pengisian Audit Program

BAB VI
HASIL DAN PEMBAHASAN

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

6.1 Verifikasi Audit Program

Verifikasi audit program ini merupakan verifikasi terhadap Prosedur dan Daftar Cek audit Pada ISO 27002 :2013 klausul Keamanan fisik dan lingkungan. Verifikasi ini dilakukan dengan cara melakukan traceback ke kontrol ISO 27002 : 2013 klausul keamanan fisik dan lingkungan yang belum disesesuaikan dengan kondisi organisasi. Pada Tabel 6.1 memaparkan hasil verifikasi yang dilakukan pada audit program

Tabel 6.1 Verifikasi Audit Program

11.1.1 *Physical Security Perimeter*		
Implementation Guidance	**Aktifitas Audit**	**Cek**
a. perimeter (denah) keamanan harus didefinisikan, dan peletakan dan kekuatan dari masing-masing perimeter harus didasarkan pada kebutuhan	1. Auditor menanyakan kepada pengadministrasian BMN terkait adanya kebutuhan perimeter untuk melindungi aset 2. Auditor menanyakan kepada Pengadministrasian BMN terkait pendefinisian perimeter keamanan pada ruang server 3. Auditor melakukan cek ketersediaan pendefinisan letak dalam denah bangunan ruang server	✓

11.1.1 *Physical Security Perimeter*		
Implementation Guidance	**Aktifitas Audit**	**Cek**
keamanan aset dalam perimeter dan hasil penilaian risiko;	4. Auditor melakukan cek ketersediaan pendefinisian konstruksi dalam denah bangunan ruang server 5. Auditor melakukan cek kesesuaian letak bangunan ruang server dengan denah bangunan ruang server 6. Auditor melakukan cek kesesuaian konstruksi bangunan dengan denah bangunan ruang server	
b. bangunan atau tempat yang berisi fasilitas pengolahan informasi secara fisik harus kedap suara ; atap eksterior, dinding dan lantai dari bangunan harus dari konstruksi yang solid dan semua pintu eksternal harus dilindungi terhadap akses yang tidak sah sesuai dengan mekanisme	7. Auditor melakukan cek terhadap bangunan terkait adanya celah pada bangunan 8. Auditor melakukan cek pada konstruksi atap, dinding dan lantai 9. Auditor melakukan cek pada pintu luar ruang server terkait adanya pengamanan akses masuk 10. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur penguncian pintu dan jendela eksternal ketika ditinggalkan	✓

11.1.1 *Physical Security Perimeter*		
Implementation Guidance	**Aktifitas Audit**	**Cek**
kontrol, (misalnya alarm dan kunci); pintu dan jendela luar harus terkunci ketika ruangan ditinggalkan;		
c. area resepsionis atau cara lain untuk mengendalikan akses fisik ke lokasi atau bangunan harus di tempat; akses ke tempat dan bangunan harus dibatasi hanya untuk orang untuk orang yang berwenang saja	11. Auditor melakukan cek terkait adanya area resepsionis 12. Auditor menanyakan kepada teknisi sarpras SI/TI terkait daftar orang yang boleh masuk keruang server	✓
d. penghalang fisik harus, dibangun untuk mencegah akses fisik tidak sah dan pencemaran lingkungan;	13. Auditor melakukan cek terkait adanya batasan fisik dengan ruangan lain	✓
e. semua pemicu kebakaran pada	14. Auditor menanyakan kepada pengadministrasian BMN	✓

11.1.1 *Physical Security Perimeter*		
Implementation Guidance	**Aktifitas Audit**	**Cek**
bangunan harus diperhitungkan, dipantau dan diuji; dalam membangun dinding harus didasarkan dengan standar regional, nasional dan internasional yang sesuai;	terkait adanya standar yang yang diacu dalam memilih konstruksi yang anti api 15. Auditor melakukan cek kesesuaian konsruksi bangunan dengan standar yang diacu	
f. Sistem pendeteksi penyusup yang cocok harus dipasang dan secara teratur diuji yang mencakup pintu dan jendela yang mungkin diakses; daerah kosong harus diamankan	16. Auditor memeriksa ketersediaan alat pendeteksi penyusup di ruang server 17. Auditor menanyakan kepada pengadministrasian BMN terkait adanya standar yang yang diacu dalam memilih alat pendeteksi 18. Auditor menanyakan kepada pengadministrasian BMN terkait adanya daftar spesifikasi alat pendeteksi 19. Auditor melakukan cek kesesuaian daftar spesifikasi alat pendeteksi penyusup dengan standar yang ada 20. Auditor melakukan cek ketersediaan ruang computer di ruang server	✓

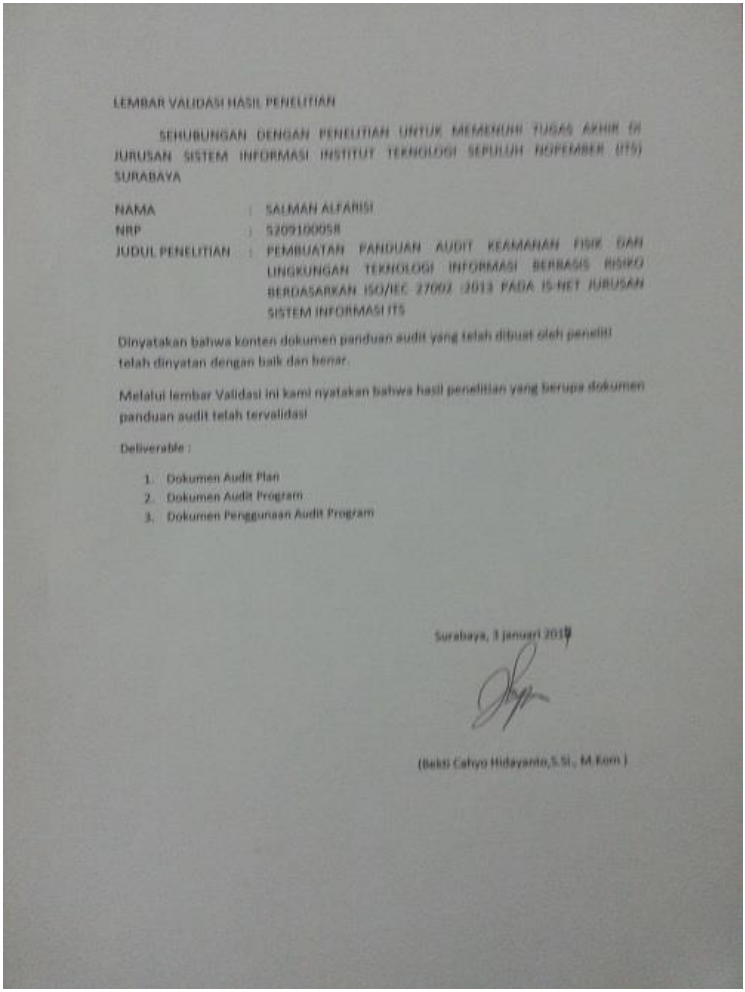
11.1.1 *Physical Security Perimeter*		
Implementation Guidance	**Aktifitas Audit**	**Cek**
g. Fasilitas pengolahan informasi yang dikelola oleh organisasi harus secara fisik dipisahkan dari yang dikelola oleh pihak eksternal	21. Auditor melakukan cek terkait pemisahan fasilitas pengolahan informasi secara fisik yang dikelola oleh organisasi dengan pihak eksternal	✓

6.2 Validasi Panduan Audit

Pada bagian ini dijelaskan mengenai proses validasi luaran penelitian yaitu dokumen panduan audit yang berisi dokumen *audit plan* dan *audit program*. Proses validasi dokumen panduan audit dilakukan dengan metode wawancara dengan pihak IS-Net yaitu dengan bapak Bekti Cahyo selaku pihak expert yang menangani ruang server di jurusan sistem informasi tujuan validasi yakni melihat kesesuaian dokumen panduan audit dengan kondisi lingkungan yang akan di audit dan kebutuhan organisasi. Dengan membuat *checklist* pemenuhan dokumen panduan audit yang telah dibuat berikut adalah aspek yang menjadi acuan dalam melakukan validasi:

1. Audit plan
2. Audit Program
3. Panduan penggunaan Audit Program

Pada gambar 6.1 berikut adalah hasil validasi yang dilakukan kepada pihak IS-Net:



LEMBAR VALIDASI HASIL PENELITIAN

SEHUBUNGAN DENGAN PENELITIAN UNTUK MEMENUHI TUGAS AKHIR DI JURUSAN SISTEM INFORMASI INSTITUT TEKNOLOGI SEPULUH NOPEMBER (ITS) SURABAYA

NAMA : SALMAN ALFARISI
NRP : 5209100058
JUDUL PENELITIAN : PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO/IEC 27002 :2013 PADA IS-NET JURUSAN SISTEM INFORMASI ITS

Dinyatakan bahwa konten dokumen panduan audit yang telah dibuat oleh peneliti telah dinyatan dengan baik dan benar.

Melalui lembar Validasi ini kami nyatakan bahwa hasil penelitian yang berupa dokumen panduan audit telah tervalidasi

Deliverable :

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

Surabaya, 3 januari 2019

(Bekti Cahyo Hidayanto,S.Si., M.Kom)

Gambar 6.1 Hasil Validasi Dokumen panduan

BAB VII
KESIMPULAN DAN SARAN

Bab ini akan menjelaskan kesimpulan yang dihasilkan dari pengerjaan tugas akhir, beserta saran yang dapat bermanfaat untuk perbaikan di penulisan selanjutnya.

7.1 Kesimpulan

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

1. Dalam dokumen *Audit Plan* terdapat jadwal audit yang terdiri dari 144 aktivitas dari 15 control objective yang di analisa
2. Dalam dokumen audit Program terdapat beberapa bagian yang berisi informasi umum, panduan penggunaan audit program serta panduan khusus. Semua yang penjelasan mengenai tata cara pengisian disajiakan dalam panduan pengunaan audit program
3. Perangkat audit yang dibuat berjumlah 15 berdasarkan setiap *control objective.* pada setiap dokumen terdiri dari beberapa poin pemeriksaan yang diuraikan dalam perangkat audit. 96 *compliance* dan 48 *substantive* yang mengacu pada ISO/IEC 27002:2013 klausul 11 dengan testing *compliance* dan testing *substantive*. Semakin banyak aktifitas pada suatu *control objective* maka semakin banyak testing *compliance* dan *substantive* nya.

7.2 Saran

Saran yang dapat diberikan oleh penulis yang diharapkan dapat dikembangkan di masa mendatang diantaranya adalah:

1. Dalam pembuatan audit plan khususnya pada penentuan estimasi waktu aktifitas audit dapat menggunakan teknik lain atau memadukan dengan teknik yang dilakukan oleh penulis, sesuai dengan apa yang dimiliki oleh masing-masing peneliti sehingga akurasi waktu pada audit plan bisa lebih baik.
2. Pada proses pembuatan prosedur audit, penelitian selanjutnya dapat lebih mendetailkan *implementation guidance* yang terdapat pada setiap kontrol, sehingga pembuatan prosedur audit lebih baik dan rinci.

DAFTAR PUSTAKA

[1] Komang Isabella Anastashia, *Teknologi informasi dalam organisasi*. Jimbaran, 2011.

[2] Budi Raharjo, *Pemanfaatan Teknologi Informasi di Perguruan Tinggi*. Bandung, 2004.

[3] Yudhis Eko Cahyo, *Pembuatan Panduan Audit Teknologi Informasi pada Proses Pengelolaan Lingkungan Fisik berbasis COBIT 5 di KPPN Surabaya II*. Surabaya: ITS, 2013.

[4] David M Griffiths, *Risk Based Internal Auditing an introduction, Version 4.4*.: www.internalaudit.biz.

[5] Krisna Harindra Dewantara, *Identifikasi, Penilaian, dan Mitigasi Risiko Keamanan Informasi B Rdasarkan Standar ISO 27001:2005 dan ISO 27002: 2013 menggunakan Metode FMEA(Studi Kasus : IS-Net)*. Surabaya, 2016.

[6] Fandy Natahiwidha, *Pembuatan Perangkat Audit Jaringan CSNET menggunakan Cobit 4.1 dan ISO 27002 pada Jurusan Sistem Informasi ITS*. Surabaya: ITS, 2010.

[7] Stephen Christian, *Pembuatan Panduan Audit Keamanan Fisik dan Lingkungan Teknologi Informasi Berbasis Risiko berdasarkan ISO 27002 : 2013 pada Direktorat Sistem Informasi Universitas Airlangga*. Surabaya, 2015.

[8] Sukrisno Agoes, *Auditing (Pemeriksaan Akuntan), Edisi 4*. Jakarta: Fakultas Ekonomi Universitas Indonesia, 2012.

[9] Alvin Arens and James K. Loebbecke, *Auditing and Assurance Services, 8th Edition*. New Jersey: Prentice Hall, 2000.

[10] dan Margareth Boh William F. Messier, *Auditing and Assurance: A Systematic Approach, 3th Edition*. USA: McGraw-Hill, 2003.

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

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

[13] Sanyoto Gondodiyoto, *Audit Sistem Informasi (+ Pendekatan CobIT)*. Jakarta: Mitra Wacana Media, 2007.

[14] Riyanarto Sarno, *Audit Sistem dan Teknologi Informasi*.: Surabaya, 2009.

[15] Valery G. Kumaat, *Internal Audit*. jakarta: Erlangga, 2011.

[16] Z. Dunil, *Risk-Based Audit : Dalam Pemeriksaan Perkreditan Bank Umum*. Jakarta: Indeks, 2006.

[17] Theodorus M Tuanakotta, *Audit Berbasis ISA*. Jakarta: Salemba Empat, 2013.

[18] Wening Insani, *Perancangan Buku Visual Cara Membuat Mainan Tradisional untuk Anak*. Surabaya: Institut Teknologi Sepuluh Nopember, 2010.

[19] Austin Community College. (2009, Nopember) Austin Community College District. [Online]. http://www.austincc.edu/audit/documents/AuditCharter091103.pdf

[20] David Mc Namee and Georgers Salim, *Risk Management, Changing the Auditor Paradigm*.: Institute Internal Auditing, 1998.

[21] Tariqullah Khan, *Manajemen Risiko*. Jakarta: PT Bumi Aksara, 2008.

[22] Amin Wijaya Tunggal, *Pedoman Pokok Opperational Auditing*. Jakarta : Harvarindo, 2012.

[23] Stoneburner G, *Risk Management Guide of Information Technology Systems*., 2002.

[24] AS/NZS ISO 31000, *Risk Management - Principles and Guidelines, 1 st Edition*. New Zealand: ISO, 2009.

[25] Melwin Syafrizal, "ISO/IEC 17799 : Standar Sistem Manajemen Keamanan Informasi," 2007.

[26] ISO/IEC 27001, *Information Technology - Security Techniques - Information Security Management System - Requirements*.

[27] Control Objective ISO 27002.pdf.

[28] Robert K. Yin, *Case Study Research Design and Method*.: Sage Publication, 1994.

[29] Project Management Institute, *A Guide to the Project Management Body of Knowledge (4th Edition)*.: Project Management Institute, 2009.

Halaman ini sengaja dikosongkan

BIODATA PENULIS

Penulis bernama lengkap Salman Al Farisi merupakan anak Pertama dari dua bersaudara yang dilahirkan di Kota Pamekasan pada tanggal 14 Maret 1991. Penulis menempuh 12 tahun masa pendidikan formal di Kota Pamekasan. Riwayat pendidikan penulis dimulai pada tahun 1997 di SDN Jungcangcang VI Pamekasan,, SMPN 1 Pamekasan pada 2003, dan SMAN 1 Pamekasan pada 2006. Pada tahun 20009, penulis meneruskan Pendidikan Tinggi Negeri di Jurusan Sistem Informasi FTIf, Institut Teknologi Sepuluh Nopember dan terdaftar dengan NRP 5209100185. Selama menjadi mahasiswa, penulis aktif sebagai anggota aktif di Himpunan Mahasiswa Sistem Informasi. Ketertarikan penulis pada bidang audit menjadikan penulis untuk memilih laboratorium Manajemen Sistem Informasi (MSI) sebagai topik dan tempat dalam menyelesaikan Tugas Akhir. Penulis pernah menjalani Kerja Praktik selama dua bulan di Bank Jatim Cabang Pamekasan. Untuk kebutuhan Penelitian dapat menghubungi penulis melalui e-mail salmanalfarisi1403@gmail.com.

Halaman ini sengaja dikosongkan

LAMPIRAN A
HASIL PENENTUAN AKTIVITAS AUDIT

Tabel A.1 Penentuan Aktifitas audit pada Control objective 11.1.1

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**
Control Objective	***Implementation Guidance***	
11.1.1 *Physical Security Perimeter*	a. perimeter (denah) keamanan harus didefinisikan, dan peletakan dan kekuatan dari masing-masing perimeter harus didasarkan pada kebutuhan keamanan aset dalam perimeter dan hasil penilaian risiko;	1. Auditor menanyakan kepada pengadministrasian BMN terkait adanya kebutuhan perimeter untuk melindungi aset 2. Auditor menanyakan kepada Pengadministrasian BMN terkait pendefinisian perimeter keamanan pada ruang server 3. Auditor melakukan cek ketersediaan pendefinisan letak dalam denah bangunan ruang server 4. Auditor melakukan cek ketersediaan pendefinisian konstruksi dalam denah

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
		bangunan ruang server 5. Auditor melakukan cek kesesuaian letak bangunan ruang server dengan denah bangunan ruang server 6. Auditor melakukan cek kesesuaian konstruksi bangunan dengan denah bangunan ruang server
	b. bangunan atau tempat yang berisi fasilitas pengolahan informasi secara fisik harus kedap suara ; atap eksterior, dinding dan lantai dari bangunan harus dari konstruksi yang solid dan semua pintu eksternal harus dilindungi terhadap akses yang tidak sah sesuai dengan mekanisme kontrol, (misalnya alarm dan	7. Auditor melakukan cek terhadap bangunan terkait adanya celah pada bangunan 8. Auditor melakukan cek pada konstruksi atap, dinding dan lantai 9. Auditor melakukan cek pada pintu luar ruang server terkait adanya pengamanan akses masuk 10. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
	kunci); pintu dan jendela luar harus terkunci ketika ruangan ditinggalkan;	penguncian pintu dan jendela eksternal ketika ditinggalkan
	c. area resepsionis atau cara lain untuk mengendalikan akses fisik ke lokasi atau bangunan harus di tempat; akses ke tempat dan bangunan harus dibatasi hanya untuk orang untuk orang yang berwenang saja	11. Auditor melakukan cek terkait adanya area resepsionis 12. Auditor menanyakan kepada teknisi sarpras SI/TI terkait daftar orang yang boleh masuk keruang server
	d. penghalang fisik harus, dibangun untuk mencegah akses fisik tidak sah dan pencemaran lingkungan;	13. Auditor melakukan cek terkait adanya batasan fisik dengan ruangan lain
	e. semua pemicu kebakaran pada bangunan harus diperhitungkan, dipantau dan diuji; dalam membangun dinding harus	14. Auditor menanyakan kepada pengadministrasian BMN terkait adanya standar yang yang diacu dalam memilih konstruksi yang anti api

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**
Control Objective	***Implementation Guidance***	
	didasarkan dengan standar regional, nasional dan internasional yang sesuai;	15. Auditor melakukan cek kesesuaian konsruksi bangunan dengan standar yang diacu
	f. Sistem pendeteksi penyusup yang cocok harus dipasang dan secara teratur diuji yang mencakup pintu dan jendela yang mungkin diakses; daerah kosong harus diamankan	16. Auditor memeriksa ketersediaan alat pendeteksi penyusup di ruang server 17. Auditor menanyakan kepada pengadministrasian BMN terkait adanya standar yang yang diacu dalam memilih alat pendeteksi 18. Auditor menanyakan kepada pengadministrasian BMN terkait adanya daftar spesifikasi alat pendeteksi 19. Auditor melakukan cek kesesuaian daftar spesifikasi alat pendeteksi penyusup dengan standar yang ada 20. Auditor melakukan cek ketersediaan ruang computer di ruang server

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**
Control Objective	***Implementation Guidance***	
	h. Fasilitas pengolahan informasi yang dikelola oleh organisasi harus secara fisik dipisahkan dari yang dikelola oleh pihak eksternal	21. Auditor melakukan cek terkait pemisahan fasilitas pengolahan informasi secara fisik yang dikelola oleh organisasi dengan pihak eksternal

Tabel A.2 Penentuan Aktifitas audit pada Control objective 11.1.2

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**
Control Objective	***Implementation Guidance***	
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. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersedian pencatatan pengunjung yang masuk ke ruang server 2. Auditor melakukan cek terhadap dokumen pencatatan terkait ketersedian penginformasian tanggal dan waktu masuk dan keluar pengunjung 3. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersedian prosedur pengawasan terhadap pengunjung 4. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur akses masuk ke ruang server kepada teknis sarpras SI/TI 5. Auditor melakukan cek terhadap

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
		dokumen pecatatan pengunjung yang masuk terkait ketersediaan indentitas pengunjung yang masuk
	a. 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 dua faktor seperti kartu akses dan PIN rahasia	6. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersesdiaan kontrol akses bagi orang yang memiliki kewenangan untuk masuk 7. Auditor melakukan cek terhadap kontrol akses yang digunakan terkait penerapan otentikasi 2 faktor
	b. Buku log fisik atau audit trail elektronik dari semua akses harus aman dijaga dan dipantau	8. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur pengelolaan log akses pengunjung yang berupa buku atau

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
		bersifat elektronik kepada teknis sarpras SI/TI 9. Auditor melakukan cek terhadap penyimpanan log akses yang berupa buku atau bersifat elektronik
	c. 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	10. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur masuk ruang server semua karyawan, kontraktor, pihak external kepada teknis sarpras SI/TI 11. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan identitas pengenal bagi semua karyawan, kontraktor, dan pihak eksternal yang memiliki akses ke ruang server 12. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersedian prosedur

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
		pelaporan terkait pengunjung yang dikawal dan yang tidak disahkan aksesnya 13. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersedian prosedur pelaporan terkait pengunjung yang tidak memakai identitas pengenal
	d. tenaga layanan pendukung dari pihak luar harus diberikan akses yang terbatas untuk mengamankan daerah atau fasilitas pengolahan informasi rahasia hanya ketika diperlukan; Akses ini harus disahkan dan dipantau;	14. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan daftar orang yang memiliki akses ke ruang server kepada teknis sarpras SI/TI 15. Auditor melakukan cek terhadap daftar orang yang memiliki akses ke ruang server terkait ketersedian hak akses bagi tenaga layanan pendukung dari luar 16. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
		prosedur akses masuk bagi tenaga layanan pendukung dari luar
	e. Hak akses untuk mengamankan area harus secara berkala dan diperbarui, dan dicabut bila diperlukan	17. Auditor melakukan cek terkait ketersediaan pembaharuan daftar hak askes bagi karyawan atau pihak ketiga yang telah putus kontrak 18. Auditor menanyakan kepada teknisi sarpras SI/TI ketersediaan daftar hak akses yang diperbaruai dan sebelum diperbarui

Tabel A.3 Penentuan Aktifitas audit pada Control objective 11.1.3

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**
Control Objective	***Implementation Guidance***	
11.1.1 *Physical Security Perimeter*	a. Fasilitas penting harus diletakkan untuk menghindari akses oleh publik	1. Auditor menanyakan kepada pengadministrasian BMN terkait aturan penentuan letak fasilitas seperti pintu dan jendela pada ruang server 2. Auditor melakukan cek kesesuaian letak pintu dan jendela dengan aturan penentuan letaknya
	b. Jika dapat diaplikasikan, bangunan harus bebas dari gangguan dan memberikan indikasi minimal tujuan mereka, dengan tidak ada tanda-tanda yang jelas, di luar atau di dalam gedung, mengidentifikasi adanya kegiatan pengolahan informasi	3. Auditor melakukan cek terkait adanya tanda keberadaan ruang server
	c. Fasilitas harus dikonfigurasi	4. Auditor melakukan cek fasilitas ruang

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
	untuk mencegah informasi atau kegiatan rahasia terlihat dan terdengar dari luar. Perisai elektromagnetik juga harus dipertimbangkan	server yang dapat terdengar atau terlihanya informasi atau kegiatan rahasia
	d. Direktori dan buku telepon internal yang menyimpan lokasi dari fasilitas pengolahan informasi rahasia tidak boleh mudah diakses siapa pun yang tidak sah	5. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya direktori dan buku telepon internal 6. Auditor melakukan cek terhadap direktori dan buku telepon internal

Tabel A.4 Penentuan Aktifitas audit pada Control objective 11.1.4

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**
Control Objective	***Implementation Guidance***	
11.1.4 Protecting against external and environmental threats	a. Saran spesialis harus diperoleh tentang cara untuk menghindari kerusakan dari kebakaran, banjir, gempa bumi, ledakan, kerusuhan sipil dan bentuk lain dari bencana alam	1. Auditor menanyakan kepada pengadministrasian BMN terkait ketersediaan pendefinisian saran spesialis tentang memberikan pengamanan ruang server 2. Auditor melakukan cek terkait ketersediaan penentuan letak dalam dokumen saran spesialis 3. Auditor melakukan cek terhadap letak ruang server terkait kesesuaian dengan dokumen saran spesialis 4. Auditor melakukan cek terkait ketersediaan penentuan konstruksi bagunan yang harus digunakan dalam dokumen saran spesialis 5. Auditor melakukan cek terhadap

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
		konstruksi bangunan ruang server terkait kesesuaian dengan dokumen saran spesialis 6. Auditor melakukan cek terkait ketersediaan penentuan alat pendukung yang harus digunakan dalam dokumen saran spesialis 7. Auditor melakukan cek terhadap alat pendukung yang ada di ruang server terkait kesesuaian dengan dokumen saran spesialis

Tabel A.5 Penentuan Aktifitas audit pada Control objective 11.1.5

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**
Control Objective	***Implementation Guidance***	
11.1.5 Working in secure areas	a. Personel harus menyadari adanya, atau kegiatan dalam, daerah aman	1. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur kerja
	b. Pekerjaan tanpa pengawasan di daerah aman harus dihindari baik untuk alasan keamanan dan untuk mencegah peluang untuk kegiatan berbahaya	2. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya peraturan yang melarang kerja tanpa pengawasan diruang server
	c. Area aman yang kosong harus secara fisik terkunci dan secara periodic diperiksa	3. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur penguncian ruang server saat ditinggalkan 4. Auditor melakukan cek terkait adanya pengamanan pada pintu di ruang server
	d. Fotografi, video, audio atau	5. Auditor menanyakan kepada teknisi

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
	peralatan rekaman lainnya, seperti kamera di perangkat mobile, seharusnya tidak diperbolehkan, kecuali diizinkan	sarpras SI/TI terkait adanya peraturan yang melarang kegiatan merekam

Tabel A.6 Penentuan Aktifitas audit pada Control objective 11.1.6

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**
Control Objective	***Implementation Guidance***	
11.1.6 Delivery and loading areas	a. Akses ke wilayah pengiriman dan penerimaan dari luar gedung harus dibatasi hanya untuk personel yang berwenang;	1. Auditor melakukan cek terkait adanya area pengiriman dan penerimaan barang di sekitar ruang server. 2. Auditor menanyakan kepada teknisi sarpras SI/TI terkait pengidentifikasiaan personel yang bertanggung jawab mengawasi di area pengiriman dan penerimaan barang
	b. Wilayah pengiriman dan pemuatan daerah harus dirancang agar pasokan dapat dimuat dan dibongkar tanpa personil pengiriman mendapatkan akses ke bagian lain dari bangunan	3. Auditor menanyakan kepada pengadministrasian BMN terkait adanya desing bangunan dan letak area pengiriman dan penerimaan barang 4. Auditor melakukan cek area pengiriman dan penerimaan barang terkait kesesuaian dengan design yang dibuat
	c. Pintu eksternal dari pengiriman	5. Auditor melakukan cek terhadap area

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
	dan pemuatan daerah harus diamankan ketika pintu internal dibuka	pengiriman dan penerimaan barang terkait keamanan akses ke gedung lain
	d. Bahan yang masuk harus diperiksa dan diperiksa untuk bahan peledak, bahan kimia atau bahan berbahaya lainnya, sebelum pindah dari wilayah pengiriman dan pemuatan	6. Auditor menanyakan kepada pengadministrasian BMN terkait adanya prosedur pemeriksaan barang 7. Auditor melakukann cek terkait adanya pencatatan pemeriksaan barang
	Bahan yang masuk harus didaftarkan sesuai dengan prosedur manajemen aset saat masuk ke area kerja	8. Auditor menanyakan kepada pengadministrasian BMN terkait adanya prosedur manajemen aset 9. Auditor melakukann cek terkait adanya pencatatan barang yang masuk ke area kerja
	e. Pengiriman masuk dan keluar harus secara fisik terpisah, jika	10. Auditor melakukan cek terkait pemisahan ruang pengiriman dengan

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
	dimungkinkan	ruang penerimaan barang
	f. Bahan yang masuk harus diperiksa untuk bukti gangguan perjalanan. Jika gangguan tersebut ditemukan harus segera dilaporkan kepada petugas keamanan	11. Auditor melakukan cek terhadap prosedur pemeriksaan barang terkait adanya pemeriksaan barang yang mengalami gangguan 12. Auditor menanyakan kepada pengadministrasian BMN terkait adanya prosedur pelaporan barang yang mengalami gangguan pengiriman

Tabel A.7 Penentuan Aktifitas audit pada Control objective 11.2.1

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**
Control Objective	***Implementation Guidance***	
11.2.1 Equipment siting and protection	a. Peralatan harus diletakkan untuk meminimalkan akses yang tidak perlu ke daerah kerja	1. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan ketentuan peletakan peralatan 2. Auditor melakukan cek terkait kesesuaian penempatan peralatan yang ada dengan dokumen ketentuan peletakan peralatan
	b. Fasilitas pengolahan informasi yang menangani data sensitif harus diposisikan hati-hati untuk mengurangi risiko informasi dilihat oleh orang yang tidak berwenang selama penggunaannya	3. Auditor melakukan cek terhadap fasilitas pengolahan informasi yang menangangi data sensitif terkait kesesuaian terhadap dokumen ketentuan peletakan
	c. Fasilitas penyimpanan harus diamankan untuk menghindari	4. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
	akses yang tidak sah	prosedur pengamanan fasilitas penyimpanan 5. Auditor melakukan cek terkait keamanan pada fasilitas penyimpanan
	d. Barang yang membutuhkan perlindungan khusus harus dijaga untuk mengurangi tingkat umum perlindungan yang diperlukan	6. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan daftar peralatan yang membutuhkan pengamanan khusus 7. Auditor melakukan cek terkait ketersediaan kebutuhan pengamanan yang ada pada daftar peralatan yang membutuhkan pengamanan khusus 8. Auditor melakukan cek terkait kesesuaian pengamanan yang ada pada peralatan yang membutuhkan pengamanan khusus terhadap kebutuhan yang ditentukan

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
	e. Kontrol harus diadopsi untuk meminimalkan risiko potensial ancaman fisik dan lingkungan, misalnya pencurian, kebakaran, bahan peledak, asap, air (atau kegagalan pasokan air), debu, getaran, efek kimia, gangguan pasokan listrik, gangguan komunikasi, radiasi elektromagnetik dan vandalisme	9. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan pengelolaan risiko yang ada diruang server terkait risiko ancaman fisik dan lingkungan 10. Auditor melakukan cek terkait kesesuaian control yang di adopsi pada dokumen pengelolaan risiko terkait risiko ancaman fisik dan lingkungan
	f. Pedoman untuk makan, minum dan merokok di dekat fasilitas pengolahan informasi harus ditetapkan	11. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur mengenai makan, minum dan merokok didekat fasilitas pengolahan informasi
	g. Kondisi lingkungan, seperti suhu dan kelembaban, harus dipantau	12. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
	untuk kondisi yang dapat mempengaruhi pengoperasian fasilitas pengolahan informasi	ketentuan suhu di ruang server 13. Auditor melakukan cek kesesuaian suhu dalam ruang server terhadap ketentuuan yang ada
	h. Perlindungan dari petir harus diterapkan untuk semua bangunan dan filter proteksi petir harus dipasang untuk semua kekuatan yang masuk dan jalur komunikasi	14. Auditor melakukan cek ketersediaan penangkal petir pada bangunan ruang server 15. Auditor melakukann cek ketersediaan pelindung elektromagnetik pada peralatan pengolahan informasi rahasia

Tabel A.8 Penentuan Aktifitas audit pada Control objective 11.2.2

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**
Control Objective	***Implementation Guidance***	
11.1.1 *Physical Security Perimeter*	a. Penyesuaian dengan spesifikasi peralatan pabrik dan persyaratan hukum lokal	1. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan kebutuhan peralatan pendukung di IS-net 2. Auditor melakukan cek kesesuaian peralatan pendukung yang ada dengan daftar kebutuhan peralatan pendukung
	b. Penilaian secara teratur untuk kapasitas mereka untuk memenuhi pertumbuhan bisnis dan interaksi dengan utilitas pendukung lainnya	3. Auditor menanyakan kepada teknis sarpras listrik terkait ketersediaan kebijakan untuk melakukan penilaian kapasitas peralatan yang ada terhadap pemenuhan pertumbuhan bisnis dan interaksi dengan peralatan pendukung lainnya 4. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan penilaian kapasitas peralatan

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
	c. Pemeriksaan dan pengujian secara teratur untuk memastikan fungsi yang tepat	5. Auditor menanyakan kepada teknis sarpras listrik terkait adanya pemeriksaan dan pengujian peralatan pendukung untuk memastikan dapat berfungsi dengan baik 6. Auditor melakukan cek terhadap dokumen pemeriksaan dan pengujian peralatan pendukung terkait kapan dilakukannya pemeriksaan dan pengujian
	d. Jika perlu, beri alarm untuk mendeteksi malfungsi	7. Auditor melakkukan cek terhadap peralatan pendukung terkait adanya pendeteksi malfungsi
	e. Jika perlu, miliki beberapa feed routing fisik yang beragam	8. Auditor menanyakan kepada teknisi sarpras listrik terkait ketersediaan kebijakan penggunaan lebih dari 1 sumber setiap peralatan pendukung

Tabel A.9 Penentuan Aktifitas audit pada Control objective 11.2.3

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**
Control Objective	***Implementation Guidance***	
11.2.3 Cabling security	a. Kabel daya dan telekomunikasi ke fasilitas pengolahan informasi harus di bawah tanah, jika memungkinkan, berikan perlindungan alternatif yang memadai	1. Auditor melakukan cek pada instalasi kabel listrik dan kabel telekomunikasi terkait penempatan kabel 2. Auditor melakukan cek terkait adanya perlindungan alternative pada kabel kepada teknis srpras listrik
	b. Kabel listrik harus dipisahkan dari kabel komunikasi untuk mencegah gangguan	3. Auditor melakukan cek terhadap kabel telekomunikasi dan kabel listrik terkait pemisahan jalur kabel
	c. Untuk sistem sensitif atau kritis lanjut kontrol untuk dipertimbangkan termasuk: 1) instalasi saluran lapis baja dan mengunci ruangan atau kotak pada titik pemeriksaan dan pemutusan;	4. Auditor menyakan kepada teknisi sarpras listrik terkait ketersediaan himbauan instalasi saluran lapis baja 5. Auditor melakukan cek terhadap kabel yang menyambung pada server terkait instalasi saluran lapis baja 6. Auditor menanyakan kepada teknisi

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
	2) menggunakan pelindung elektromagnetik untuk melindungi kabel; 3) inisiasi peembersihan teknis dan pemeriksaan fisik untuk perangkat yang tidak sah yang melekat pada kabel; 4) akses dikendalikan untuk patch panel dan ruang kabel.	sarpras listrik terkait adanya himbauan penguncian kotak inspeksi dan pemutusan listrik 7. Auditor menanyakan kepada teknisi sarpras listrik terkait adanya himbauan instalasi kabel dengan penggunaan pelindung elektromagnetik 8. Auditor melakukan cek terhadap kabel yang menyambung pada server terkait penggunaan pelindung elektromagnetik 9. Auditor menayakan kepada teknisi sarpras listrik terkait ketersedian prosedur pengendalian akses ke patch panel dan ruangan kabel 10. Auditor melakukan cek ke patch panel dan ruangan kabel terkait adanya penguncian patch panel atau ruangan

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
		kabel

Tabel A.10 Penentuan Aktifitas audit pada Control objective 11.2.4

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**
Control Objective	***Implementation Guidance***	
11.2.4 Equipment maintenance	a. Peralatan harus dipelihara sesuai dengan interval servis pemasok yang dianjurkan dan spesifikasi	1. Auditor menayakan kepada Teknisi srarpras SI/TI terkait adanya anjuran pemeliharan peralatan dari pemasok 2. Auditor menanyakan kepada srarpras SI/TI terkait ketersediaan pencatatan pemeliharaan peralatan 3. Auditor menanyakan kepada Teknisi srarpras SI/TI terkait adanya pencatatan pemeliharaan peralatan yang dianjurkan oleh pemasok
	b. Semua kebutuhan perawatan yang dianjurkan oleh kebijakan asuransi harus dipenuhi	4. Auditor menanyakan kepada srarpras SI/TI terkait adanya kebijakan asuransi mengenai kebutuhan pemeliharaan peralatan 5. Auditor menanyakan kepada Teknisi srarpras SI/TI terkait adanya pencatatan

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
		pemeliharaan peralatan yang dianjurkan oleh pihak asuransi
	c. Hanya personil pemeliharaan yang berwenang yang harus melakukan perbaikan dan layanan peralatan	6. Auditor menanyakan kepada srarpras SI/TI terkait kewenangan proses pemeliharaan peralatan 7. Auditor melakukan cek terhadap pencatatan pemeliharaan peralatan terkait orang yang berwenang
	d. Catatan perkiraan kesalahan atau kesalahan aktual, dan semua pemeliharaan preventif dan korektif harus disimpan	8. Auditor menanyakan kepada srarpras SI/TI terkait pemeriksaan peralatan setelah dilakukan pemeliharaan 9. Auditor melakukan cek terhadap pencatatan pemeliharaan peralatan terkait pemeriksaan peralatan setelah dilakukan pemeliharaan
	e. Pengendalian yang tepat harus dilaksanakan bila peralatan	10. Auditor menanyakan kepada srarpras SI/TI terkait penjadwalan pemeliharaan

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
	dijadwalkan untuk pemeliharaan, dengan mempertimbangkan apakah perawatan ini dilakukan oleh personel	peralatan 11. Auditor menanyakan kepada srarpras SI/TI terkait ketersediaan kebijakan proses pemeliharaan yang dilakukan di tempat (ruang server) 12. Auditor menanyakan kepada srarpras SI/TI terkait ketersediaan kebijakan pemeliharaan yang akan menggunakan jasa ekternal 13. Auditor menanyakan kepada srarpras SI/TI terkait ketersediaan prosedur penghapusan informasi rahasia pada peralatan yang akan dilakukan pemeliharaan

Tabel A.11 Penentuan Aktifitas audit pada Control objective 11.2.5

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**
Control Objective	***Implementation Guidance***	
11.1.1 *Physical Security Perimeter*	a. Karyawan dan pihak eksternal yang memiliki otoritas untuk mengizinkan peminjaman aset harus diidentifikasi	1. Auditor menanyakan kepada teknisi sarpras SI/TI terkait pengidentifikasian orang yang memiliki tanggung jawab memberikan izin peminjaman aset
	b. Batas waktu peminjaman aset harus ditetapkan dan kembali diverifikasi untuk kepatuhan	2. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur peminjaman aset TI 3. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya pencatatan peminjaman aset 4. Auditor melakukan cek terkait adanya proses verifikasi batas waktu peminjaman set dalam prosedur peminjaman aset 5. Auditor melakukan cek pada pencatatan peminjaman aset terkait adanya checklist

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
		verifikasi
	c. Bila perlu, aset harus dicatat sebagai aset yang dipinjam dan dicatat ketika kembali	6. Auditor melakukan cek pada dokumen pencatatan peminjaman aset terkait adanya pencatatan barang ketika dikembalikan
	d. Identitas, peran dan afiliasi dari siapa saja yang menangani atau menggunakan aset harus didokumentasikan dan dokumentasi ini kembali dengan peralatan, informasi atau perangkat lunak	7. Auditor melakukan cek pada pencatatan peminjaman aset terkait adanya informasi identitas, jabatan, dan tujuan

Tabel A.12 Penentuan Aktifitas audit pada Control objective 11.2.6

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**
Control Objective	***Implementation Guidance***	
11.2.6 Security of equipment and assets off-premises	a. Peralatan dan media diambil dari tempat tidak boleh dibiarkan tanpa pengawasan di tempat umum	1. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya kebijakan penggunaan peralatan diluar organisasi 2. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya pencatatan penggunaan peralan dan media diluar ruang server
	b. Instruksi produsen untuk melindungi peralatan harus diamati setiap saat, misalnya perlindungan terhadap paparan medan elektromagnetik yang kuat	3. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya instruksi produsen mengenai pengamanan peralatan yang dipakai diluar
	c. Kontrol untuk lokasi *off-site*, seperti rumah kerja, teleworking dan situs sementara harus ditentukan oleh penilaian risiko	4. Auditor menanyakan kepada teknisi sarpras SI/TI terkait pengelolaan risiko terhadap penggunaan peralatan dan media diluar organisasi

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
	dan control cocok diterapkan sebagaimana mestinya, misalnya lemari arsip dikunci, kebijakan meja yang jelas, kontrol akses untuk komputer dan komunikasi yang aman dengan kantor	
	d. Ketika peralatan *off-site* ditransfer antara individu-individu yang berbeda atau pihak eksternal, log harus dipertahankan yang mendefinisikan lacak balak pada peralatan termasuk setidaknya nama dan organisasi dari orang-orang yang bertanggung jawab untuk peralatan	5. Auditor menayakan kepada teknisi sarpras SI/TI terkait adanya prosedur pengalihan peralatan yang digunakan diluar ruang server 6. Auditor melakukan cek dokumen pencatatan terkait adanya pendefiniasn nama dan organisasi yang bertanggunng jawab pada peralatan

Tabel A.13 Penentuan Aktifitas audit pada Control objective 11.2.7

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**
Control Objective	***Implementation Guidance***	
11.2.7 Secure disposal or re-use of equipment	a. Peralatan harus diverifikasi untuk memastikan apakah media penyimpanan yang terkandung sebelum dibuang atau digunakan kembali.	1. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersedian prosedur penghapusan informasi pada media penyimpanan 2. Auditor melakukan cek terkait adanya proses verifikasi sebelum dibuang atau digunakan kembali terhadap media penyimpanan

	b. Media penyimpanan yang berisi informasi rahasia atau hak cipta harus secara fisik dihancurkan atau informasinya harus dihancurkan, dihapus atau ditimpa menggunakan teknik untuk membuat informasi asli tidak dapat diambil kemabali daripada menggunakan standar menghapus atau fungsi Format	3. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur yang mengatur teknik penghapusan dan penimpaan pada media penyimpanan 4. Auditor melakukan cek kesesuaian teknik penghapusan atau penimpaan yang digunakan oleh karyawan terhadap prosedur yang ada

Tabel A.14 Penentuan Aktifitas audit pada Control objective 11.2.8

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**
Control Objective	***Implementation Guidance***	
11.2.8 Unattended user equipment	a. Mengakhiri sesi aktif ketika selesai, kecuali bisa diamankan oleh mekanisme penguncian yang tepat, misalnya dilindungi password screen saver	1. Auditor menanyakan kepada teknis sarpras SI/TI terkait ketersediaan prosedur perlindungan perlatan yang tidak diawasi 2. Auditor melakukan cek terhadap komputer teknis sarpras SI/TI terkait penggunaan password screean saver
	b. Log-off dari aplikasi atau layanan jaringan ketika tidak lagi dibutuhkan	3. Auditor melakukan cek terhadap komputer yang digunakan teknis sarpras SI/TI terkait log-off dari aplikasi atau layanan jaringan ketika tidak digunakan
	c. Mengamankan komputer atau perangkat mobile dari penggunaan yang tidak sah oleh kunci kunci atau kontrol yang setara, misalnya akses password,	4. Auditor melakukan cek terhadap computer atau handphone yang digunakan teknis sarpras SI/TI terkait ketersedian penggunaan password

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
	jika tidak digunakan	

Tabel A.15 Penentuan Aktifitas audit pada Control objective 11.2.9

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**
Control Objective	***Implementation Guidance***	
11.2.9 Clear desk and clear screen policy	a. Informasi bisnis yang sensitif atau kritis, misalnya di atas kertas atau media penyimpanan elektronik, harus terkunci (idealnya dalam bentuk yang aman atau lemari atau lainnya furnitur keamanan) bila tidak diperlukan, terutama ketika kantor dikosongkan.	1. Auditor menanyakan kepada teknis sarpras SI/TI terkait ketersediaan prosedur penyimpanan informasi bisnis yang kritis atau sensitive yang berupa dokumen kertas atau media penyimpanan elektronik 2. Auditor melakukan cek ke dalam ruang server terkait ketersediaan lemari penyimpanan dokumen yang berisi informasi kritis 3. Auditor melakukan cek terdahap keamanan lemari penyimpanan dokumen yang berisi informasi kritis 4. Auditor melakukan cek ke ruang server terkait ketersediaan pengaman pada media penyimpanan elektronik

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
	b. Komputer dan terminal harus dibiarkan log off atau dilindungi dengan layar dan keyboard dengan penguncian password, mekanisme otentikasi pengguna tanda atau serupa ketika tanpa pengawasan dan harus dilindungi oleh kunci kunci, password atau kontrol lain jika tidak digunakan	5. Auditor melakukan cek ketersediaan prosedur penguncian komputer saat tidak digunakaan 6. Auditor melakukan cek terhadap komputer yang digunakan teknisi sarpras SI/TI diruang server terkait penggunaan password pada computer
	c. Penggunaan yang tidak sah dari mesin fotokopi dan teknologi reproduksi lainnya (misalnya scanner, kamera digital) harus dicegah	7. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan daftar pengguna peralatan seperti mesin fotokopi, scanner dan kamera digital di ruang server 8. Auditor menanyakan kepada teknisi sarpras SI/TI ketersediaan peraturan yang melarang penggunaan peralatan seperti

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit
Control Objective	***Implementation Guidance***	
		mesin fotokopi, scanner dan kamera di ruang server selain daftar pengguna
	d. media yang mengandung informasi sensitif atau rahasia harus dihapus dari printer segera.	9. Auditor menanyakan kepada teknisi sarpras SI/TI kebijakan penghapusan informasi sensitif atau rahasia dari printer

LAMPIRAN B
JADWAL KEGIATAN AUDIT

Pada Lampiran ini Memberikan Contoh isi dari *Audit Plan.* Bagian *Audit Plan* yang akan diberikan adalah bagian *Gantt Chart* yang mencakup seluruh aktifitas audit. Pada Tabel B.1 adalah Tabel WBS.

Tabel B.1 Tabel WBS

No. WBS	Aktifitas Audit	Durasi	Start	Finish	Predecessors	Resource Name
1.	Auditor menanyakan kepada pengadministrasian BMN terkait adanya kebutuhan perimeter(Denah) untuk melindungi aset	6,6 mins	Tue 02/01/18	Tue 02/01/18		Pengelola Administrasi BMN
2.	Auditor menanyakan kepada Pengadministrasian BMN terkait pendefinisian perimeter(Denah) keamanan pada ruang server	6,6 mins	Tue 02/01/18	Tue 02/01/18	1	Pengelola Administrasi BMN
3.	Auditor melakukan cek ketersediaan letak perimeter dalam denah bangunan ruang server	6,6 mins	Tue 02/01/18	Tue 02/01/18	2	Pengelola Administrasi BMN
4.	Auditor melakukan cek ketersediaan pendefinisian konstruksi perimeter dalam denah bangunan ruang server	6,6 mins	Tue 02/01/18	Tue 02/01/18	3	Pengelola Administrasi BMN
5.	Auditor menanyakan kepada pengadministrasian BMN terkait adanya standar yang yang diacu dalam memilih konstruksi yang anti api	6,6 mins	Tue 02/01/18	Tue 02/01/18	4	Pengelola Administrasi BMN
6.	Auditor menanyakan kepada pengadministrasian BMN terkait adanya standar yang yang diacu dalam memilih alat pendeteksi	6,6 mins	Tue 02/01/18	Tue 02/01/18	5	Pengelola Administrasi BMN
7.	Auditor menanyakan kepada pengadministrasian BMN terkait adanya daftar spesifikasi alat pendeteksi	6,6 mins	Tue 02/01/18	Tue 02/01/18	6	Pengelola Administrasi BMN
8.	Auditor menanyakan kepada pengadministrasian BMN terkait aturan penentuan letak fasilitas seperti pintu dan jendela pada ruang server	6,6 mins	Tue 02/01/18	Tue 02/01/18	7	Pengelola Administrasi BMN
9.	Auditor menanyakan kepada pengadministrasian BMN terkait ketersediaan pendefinisian saran spesialis tentang memberikan pengamanan ruang server	6,6 mins	Tue 02/01/18	Tue 02/01/18	8	Pengelola Administrasi BMN
10.	Auditor melakukan cek terkait ketersediaan penentuan letak dalam dokumen saran spesialis	6,6 mins	Tue 02/01/18	Tue 02/01/18	9	Pengelola Administrasi BMN
11.	Auditor melakukan cek terkait ketersediaan penentuan konstruksi bagunan yang harus digunakan dalam dokumen saran spesialis	6,6 mins	Tue 02/01/18	Tue 02/01/18	10	Pengelola Administrasi BMN
12.	Auditor melakukan cek terkait ketersediaan penentuan alat pendukung	6,6 mins	Tue	Tue	11	Pengelola Administrasi

	yang harus digunakan dalam dokumen saran spesialis		02/01/18	02/01/18		BMN
13.	Auditor menanyakan kepada pengadministrasian BMN terkait adanya desing bangunan dan letak area pengiriman dan penerimaan barang	4,6 mins	Tue 02/01/18	Tue 02/01/18	12	Pengelola Administrasi BMN
14.	Auditor menanyakan kepada pengadministrasian BMN terkait adanya prosedur pemeriksaan barang	6,6 mins	Tue 02/01/18	Tue 02/01/18	13	Pengelola Administrasi BMN
15.	Auditor menanyakan kepada pengadministrasian BMN terkait adanya prosedur manajemen aset	6,6 mins	Tue 02/01/18	Tue 02/01/18	14	Pengelola Administrasi BMN
16.	Auditor menanyakan kepada pengadministrasian BMN terkait adanya prosedur pelaporan barang yang mengalami gangguan pengiriman	6,6 mins	Tue 02/01/18	Tue 02/01/18	15	Pengelola Administrasi BMN
17.	Auditor menanyakan kepada teknis sarpras listrik terkait ketersediaan kebijakan penilaian kapasitas peralatan yang ada terhadap pemenuhan pertumbuhan bisnis dan interaksi dengan peralatan pendukung lainnya	6,6 mins	Tue 02/01/18	Tue 02/01/18	16	Teknisi Sarpras Listrik
18.	Auditor menanyakan kepada teknisi sarpras Listrik terkait ketersediaan penilaian kapasitas peralatan	6,6 mins	Tue 02/01/18	Tue 02/01/18	17	Teknisi Sarpras Listrik
19.	Auditor menanyakan kepada teknis sarpras listrik terkait adanya pemeriksaan dan pengujian peralatan pendukung untuk memastikan dapat berfungsi dengan baik	6,6 mins	Tue 02/01/18	Tue 02/01/18	18	Teknisi Sarpras Listrik
20.	Auditor menanyakan kepada teknisi sarpras listrik terkait ketersediaan kebijakan penggunaan lebih dari 1 sumber setiap peralatan pendukung	6,6 mins	Tue 02/01/18	Tue 02/01/18	19	Teknisi Sarpras Listrik
21.	Auditor melakukan cek terkait adanya perlindungan alternative pada kabel kepada teknis sarpras listrik	6,6 mins	Tue 02/01/18	Tue 02/01/18	20	Teknisi Sarpras Listrik
22.	Auditor menanyakan kepada teknisi sarpras listrik terkait ketersediaan prosedur penguncian kotak inspeksi dan pemutusan listrik	6,6 mins	Tue 02/01/18	Tue 02/01/18	21	Teknisi Sarpras Listrik
23.	Auditor menanyakan kepada teknisi sarpras listrik terkait ketersediaan prosedur instalasi kabel dengan penggunaan pelindung elektromagnetik	6,6 mins	Tue 02/01/18	Tue 02/01/18	22	Teknisi Sarpras Listrik
24.	Auditor menayakan kepada teknisi sarpras listrik terkait ketersedian prosedur pengendalian akses ke patch panel dan ruangan kabel	6,6 mins	Tue 02/01/18	Tue 02/01/18	23	Teknisi Sarpras Listrik
25.	Auditor melakukan cek kesesuaian letak bangunan ruang server dengan dokumen arsitektur bangunan	6,6 mins	Tue 02/01/18	Tue 02/01/18	24	Teknisi Sarpras SI/TI
26.	Auditor melakukan cek kesesuaian konstruksi bangunan dengan dokumen arsitektur bangunan	6,6 mins	Tue 02/01/18	Tue 02/01/18	25	Teknisi Sarpras SI/TI
27.	Auditor melakukan cek terhadap bangunan terkait adanya celah pada	6,6 mins	Tue	Tue	26	Teknisi Sarpras SI/TI

	bangunan		02/01/18	02/01/18		
28.	Auditor melakukan cek pada konstruksi atap, dinding dan lantai	6,6 mins	Tue 02/01/18	Tue 02/01/18	27	Teknisi Sarpras SI/TI
29.	Auditor melakukan cek pada pintu luar ruang server terkait adanya pengamanan akses masuk	6,6 mins	Tue 02/01/18	Tue 02/01/18	28	Teknisi Sarpras SI/TI
30.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur penguncian pintu dan jendela eksternal ketika ditinggalkan	6,6 mins	Tue 02/01/18	Tue 02/01/18	29	Teknisi Sarpras SI/TI
31.	Auditor melakukan cek terkait adanya area resepsionis	6,6 mins	Tue 02/01/18	Tue 02/01/18	30	Teknisi Sarpras SI/TI
32.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait daftar orang yang boleh masuk keruang server	6,6 mins	Tue 02/01/18	Tue 02/01/18	31	Teknisi Sarpras SI/TI
33.	Auditor melakukan cek terkait adanya batasan fisik dengan ruangan lain	6,6 mins	Tue 02/01/18	Tue 02/01/18	32	Teknisi Sarpras SI/TI
34.	Auditor melakukan cek kesesuaian konsruksi bangunan dengan standar yang diacu	6,6 mins	Tue 02/01/18	Tue 02/01/18	33	Teknisi Sarpras SI/TI
35.	Auditor memeriksa ketersediaan alat pendeteksi penyusup di ruang server	6,6 mins	Tue 02/01/18	Tue 02/01/18	34	Teknisi Sarpras SI/TI
36.	Auditor melakukan cek kesesuaian daftar spesifikasi alat pendeteksi penyusup dengan standar yang ada	6,6 mins	Tue 02/01/18	Tue 02/01/18	35	Teknisi Sarpras SI/TI
37.	Auditor melakukan cek ketersediaan ruang komputer	6,6 mins	Tue 02/01/18	Tue 02/01/18	36	Teknisi Sarpras SI/TI
38.	Auditor melakukan cek terkait pemisahan fasilitas pengolahan informasi secara fisik yang dikelola oleh organisasi dengan pihak eksternal	6,6 mins	Tue 02/01/18	Tue 02/01/18	37	Teknisi Sarpras SI/TI
39.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersedian pencatatan pengunjung yang masuk ke ruang server	6,6 mins	Tue 02/01/18	Tue 02/01/18	38	Teknisi Sarpras SI/TI
40.	Auditor melakukan cek terhadap dokumen pencatatan terkait ketersedian penginformasian tanggal dan waktu maktu masuk pengunjung	6,6 mins	Tue 02/01/18	Tue 02/01/18	39	Teknisi Sarpras SI/TI
41.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersedian prosedur pengawasan terhadap pengunjung	6,6 mins	Tue 02/01/18	Tue 02/01/18	40	Teknisi Sarpras SI/TI
42.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur akses masuk ke ruang server	6,6 mins	Tue 02/01/18	Tue 02/01/18	41	Teknisi Sarpras SI/TI
43.	Auditor melakukan cek terhadap dokumen pecatatan pengunjung yang	6,6 mins	Tue	Tue	42	Teknisi Sarpras SI/TI

	masuk terkait ketersediaan indentitas pengunjung yang masuk		02/01/18	02/01/18		
44.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersesdiaan kontrol akses bagi orang yang memiliki kewenangan untuk masuk	6,6 mins	Tue 02/01/18	Tue 02/01/18	43	Teknisi Sarpras SI/TI
45.	Auditor melakukan cek terhadap kontrol akses yang digunakan terkait penerapan otentikasi 2 faktor	6,6 mins	Tue 02/01/18	Tue 02/01/18	44	Teknisi Sarpras SI/TI
46.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur pe pengelolaan log akses pengunjung yang berupa buku atau bersifat elektronik	6,6 mins	Tue 02/01/18	Tue 02/01/18	45	Teknisi Sarpras SI/TI
47.	Auditor melakukan cek terhadap penyimpanan log akses yang berupa buku atau bersifat elektronik	6,6 mins	Tue 02/01/18	Tue 02/01/18	46	Teknisi Sarpras SI/TI
48.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur masuk ruang server semua karyawan, kontraktor, pihak external kepada teknis sarpras SI/TI	6,6 mins	Tue 02/01/18	Tue 02/01/18	47	Teknisi Sarpras SI/TI
49.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan identitas pengenal bagi semua karyawan, kontraktor, dan pihak eksternal yang memiliki akses ke ruang server	6,6 mins	Tue 02/01/18	Tue 02/01/18	48	Teknisi Sarpras SI/TI
50.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersedian prosedur pelaporan terkait pengunjung yang dikawal dan yang tidak disahkan aksesnya	6,6 mins	Tue 02/01/18	Tue 02/01/18	49	Teknisi Sarpras SI/TI
51.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersedian prosedur pelaporan terkait pengunjung yang tidak memakai identitas pengenal	6,6 mins	Tue 02/01/18	Tue 02/01/18	50	Teknisi Sarpras SI/TI
52.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan daftar orang yang memiliki akses ke ruang server	6,6 mins	Tue 02/01/18	Tue 02/01/18	51	Teknisi Sarpras SI/TI
53.	Auditor melakukan cek terhadap daftar orang yang memiliki akses ke ruang server terkait ketersedian hak akses bagi tenaga layanan pendukung dari luar	6,6 mins	Tue 02/01/18	Tue 02/01/18	52	Teknisi Sarpras SI/TI
54.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur akses masuk bagi tenaga layanan pendukung dari luar	6,6 mins	Tue 02/01/18	Tue 02/01/18	53	Teknisi Sarpras SI/TI
55.	Auditor menanyakan terkait ketersediaan prosedur pembaharuan daftar hak askes bagi karyawan atau pihak ketiga yang telah putus kontrak	6,6 mins	Tue 02/01/18	Tue 02/01/18	54	Teknisi Sarpras SI/TI
56.	Auditor menanyakan kepada teknisi sarpras SI/TI ketersediaan daftar hak akses yang diperbaruai dan sebelum diperbarui	6,6 mins	Tue 02/01/18	Tue 02/01/18	55	Teknisi Sarpras SI/TI

57.	Auditor melakukan cek kesesuaian letak pintu dan jendela dengan aturan penentuan letaknya	6,6 mins	Tue 02/01/18	Tue 02/01/18	56	Teknisi Sarpras SI/TI
58.	Auditor melakukan cek terkait adanya tanda keberadaan ruang server	6,6 mins	Tue 02/01/18	Tue 02/01/18	57	Teknisi Sarpras SI/TI
59.	Auditor melakukan cek fasilitas ruang server yang dapat terdengar atau terlihanya informasi atau kegiatan rahasia	6,6 mins	Tue 02/01/18	Tue 02/01/18	58	Teknisi Sarpras SI/TI
60.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya direktori dan buku telepon internal	6,6 mins	Tue 02/01/18	Tue 02/01/18	59	Teknisi Sarpras SI/TI
61.	Auditor melakukan cek terhadap pengaman direktori dan buku telepon internal	6,6 mins	Tue 02/01/18	Tue 02/01/18	60	Teknisi Sarpras SI/TI
62.	Auditor melakukan cek terhadap letak ruang server terkait kesesuaian dengan dokumen saran spesialis	6,6 mins	Tue 02/01/18	Tue 02/01/18	61	Teknisi Sarpras SI/TI
63.	Auditor melakukan cek terhadap konstruksi bangunan ruang server terkait kesesuaian dengan dokumen saran spesialis	6,6 mins	Tue 02/01/18	Tue 02/01/18	62	Teknisi Sarpras SI/TI
64.	Auditor melakukan cek terhadap alat pendukung yang ada di ruang server terkait kesesuaian dengan dokumen saran spesialis	6,6 mins	Tue 02/01/18	Tue 02/01/18	63	Teknisi Sarpras SI/TI
65.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur kerja	6,6 mins	Tue 02/01/18	Tue 02/01/18	64	Teknisi Sarpras SI/TI
66.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur yang melarang kerja tanpa pengawasan diruang server	6,6 mins	Tue 02/01/18	Tue 02/01/18	65	Teknisi Sarpras SI/TI
67.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur penguncian ruang server saat ditinggalkan	6,6 mins	Tue 02/01/18	Tue 02/01/18	66	Teknisi Sarpras SI/TI
68.	Auditor melakukan cek terkait adanya pengamanan pada pintu di ruang server	6,6 mins	Tue 02/01/18	Tue 02/01/18	67	Teknisi Sarpras SI/TI
69.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya peraturan yang melarang kegiatan merekam	6,6 mins	Tue 02/01/18	Tue 02/01/18	68	Teknisi Sarpras SI/TI
70.	Auditor melakukan cek terkait adanya area pengiriman dan penerimaan barang di sekitar ruang server	6,6 mins	Tue 02/01/18	Tue 02/01/18	69	Teknisi Sarpras SI/TI
71.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait pengidentifikasiaan personel yang bertanggung jawab mengawasi di area pengiriman dan penerimaan barang	6,6 mins	Tue 02/01/18	Tue 02/01/18	70	Teknisi Sarpras SI/TI
72.	Auditor melakukan cek area pengiriman dan penerimaan barang terkait	6,6 mins	Tue	Tue	71	Teknisi Sarpras SI/TI

	kesesuaian dengan design yang dibuat		02/01/18	02/01/18		
73.	Auditor melakukan cek terhadap area pengiriman dan penerimaan barang terkait keamanan akses ke gedung lain	6,6 mins	Tue 02/01/18	Tue 02/01/18	72	Teknisi Sarpras SI/TI
74.	Auditor melakukann cek terkait adanya pencatatan pemeriksaan barang	6,6 mins	Tue 02/01/18	Wed 03/01/18	73	Teknisi Sarpras SI/TI
75.	Auditor melakukann cek terkait adanya pencatatan barang yang masuk ke area kerja	6,6 mins	Wed 03/01/18	Wed 03/01/18	74	Teknisi Sarpras SI/TI
76.	Auditor melakukan cek terkait pemisahan ruang pengiriman dengan ruang penerimaan barang	6,6 mins	Wed 03/01/18	Wed 03/01/18	75	Teknisi Sarpras SI/TI
77.	Auditor melakukan cek terhadap prosedur pemeriksaan barang terkait adanya pemeriksaan barang yang mengalami gangguan	6,6 mins	Wed 03/01/18	Wed 03/01/18	76	Teknisi Sarpras SI/TI
78.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan ketentuan peletakan peralatan	6,6 mins	Wed 03/01/18	Wed 03/01/18	77	Teknisi Sarpras SI/TI
79.	Auditor melakukan cek terkait kesesuai penempatan peralatan yang ada dengan dokumen ketentuan peletakan peralatan	6,6 mins	Wed 03/01/18	Wed 03/01/18	78	Teknisi Sarpras SI/TI
80.	Auditor melakukan cek terhadap fasilitas pengolahan informasi yang menangangi data sensitif terkait kesesuaian terhadap dokumen ketentuan peletakan	6,6 mins	Wed 03/01/18	Wed 03/01/18	79	Teknisi Sarpras SI/TI
81.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur pengamanan fasilitas penyimpanan	6,6 mins	Wed 03/01/18	Wed 03/01/18	80	Teknisi Sarpras SI/TI
82.	Auditor melakukan cek terkait keamanan fasilitas penyimpanan	6,6 mins	Wed 03/01/18	Wed 03/01/18	81	Teknisi Sarpras SI/TI
83.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan daftar peralatan yang membutuhkan pengamanan khusus	6,6 mins	Wed 03/01/18	Wed 03/01/18	82	Teknisi Sarpras SI/TI
84.	Auditor melakukan cek terkait ketersediaan kebutuhan pengamanan yang ada pada daftar peralatan yang membutuhkan pengamanan khusus	6,6 mins	Wed 03/01/18	Wed 03/01/18	83	Teknisi Sarpras SI/TI
85.	Auditor melakukan cek terkait kesesuaian pengamanan yang ada pada peralatan yang membutuhkan pengamanan khusus terhadap kebutuhan yang ditentukan	6,6 mins	Wed 03/01/18	Wed 03/01/18	84	Teknisi Sarpras SI/TI
86.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan pengelolaan risiko yang ada diruang server terkait risiko ancaman fisik dan lingkungan	6,6 mins	Wed 03/01/18	Wed 03/01/18	85	Teknisi Sarpras SI/TI

87.	Auditor melakukan cek terkait kesesuaian control yang di adopsi pada dokumen pengelolaan risiko terkait risiko ancaman fisik dan lingkungan	6,6 mins	Wed 03/01/18	Wed 03/01/18	86	Teknisi Sarpras SI/TI
88.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur mengenai makan, minum dan merokok didekat fasilitas pengolahan informasi	6,6 mins	Wed 03/01/18	Wed 03/01/18	87	Teknisi Sarpras SI/TI
89.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan ketentuan suhu di ruang server	6,6 mins	Wed 03/01/18	Wed 03/01/18	88	Teknisi Sarpras SI/TI
90.	Auditor melakukan cek kesesuaian suhu dalam ruang server terhadap ketentuuan yang ada	6,6 mins	Wed 03/01/18	Wed 03/01/18	89	Teknisi Sarpras SI/TI
91.	Auditor melakukan cek ketersediaan penangkal petir pada bangunan ruang server	4,6 mins	Wed 03/01/18	Wed 03/01/18	90	Teknisi Sarpras SI/TI
92.	Auditor melakukann cek ketersediaan pelindung elektromagnetik pada peralatan pengolahan informasi rahasia	6,6 mins	Wed 03/01/18	Wed 03/01/18	91	Teknisi Sarpras SI/TI
93.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan ketentuan kebutuhan peralatan pendukung di IS-net	6,6 mins	Wed 03/01/18	Wed 03/01/18	92	Teknisi Sarpras SI/TI
94.	Auditor melakukan cek kesesuaian peralatan pendukung yang ada dengan daftar kebutuhan peralatan pendukung	6,6 mins	Wed 03/01/18	Wed 03/01/18	93	Teknisi Sarpras SI/TI
95.	Auditor melakukan cek terhadap dokumen pemeriksaan dan pengujian peralatan pendukung	6,6 mins	Wed 03/01/18	Wed 03/01/18	94	Teknisi Sarpras SI/TI
96.	Auditor melakkukan cek terhadap peralatan pendukung terkait mendeteksi malfungsi	6,6 mins	Wed 03/01/18	Wed 03/01/18	95	Teknisi Sarpras SI/TI
97.	Auditor melakukan cek pada instalasi kabel listrik dan kabel telekomunikasi terkait penempatan kabel	6,6 mins	Wed 03/01/18	Wed 03/01/18	96	Teknisi Sarpras SI/TI
98.	Auditor melakukan cek terhadap kabel telekomunikasi dan kabel listrik	6,6 mins	Wed 03/01/18	Wed 03/01/18	97	Teknisi Sarpras SI/TI
99.	auditor menyakan kepada teknisi sarpras listrik terkait ketersediaan prosedur instalasi saluran lapis baja	6,6 mins	Wed 03/01/18	Wed 03/01/18	98	Teknisi Sarpras SI/TI
100.	Auditor melakukan cek terhadap kabel yang menyambung pada server terkait instalasi saluran lapis baja	6,6 mins	Wed 03/01/18	Wed 03/01/18	99	Teknisi Sarpras SI/TI
101.	Auditor melakukan cek terhadap kabel yang menyambung pada server terkait penggunaan pelindung elektromagnetik	6,6 mins	Wed 03/01/18	Wed 03/01/18	100	Teknisi Sarpras SI/TI
102.	Auditor menayakan kepada Teknisi srarpras SI/TI terkait adanya anjuran	6,6 mins	Wed	Wed	101	Teknisi Sarpras SI/TI

	pemeliharan peralatan dari pemasok		03/01/18	03/01/18		
103.	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait ketersediaan pencatatan pemeliharaan peralatan	6,6 mins	Wed 03/01/18	Wed 03/01/18	102	Teknisi Sarpras SI/TI
104.	Auditor melakukan cek terhadap pencatatan pemeliharaan terkait pemeliharaan peralatan yang dianjurkan oleh pemasok	6,6 mins	Wed 03/01/18	Wed 03/01/18	103	Teknisi Sarpras SI/TI
105.	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait adanya kebijakan asuransi mengenai kebutuhan pemeliharaan peralatan	6,6 mins	Wed 03/01/18	Wed 03/01/18	104	Teknisi Sarpras SI/TI
106.	Auditor melakukan cek terhadap pencatatan pemeliharaan terkait kebutuhan pemeliharaan yang terdapat pada kebijakan asuransi	6,6 mins	Wed 03/01/18	Wed 03/01/18	105	Teknisi Sarpras SI/TI
107.	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait kewenangan proses pemeliharaan peralatan	6,6 mins	Wed 03/01/18	Wed 03/01/18	106	Teknisi Sarpras SI/TI
108.	Auditor melakukan cek terhadap pencatatan pemeliharaan peralatan terkait orang yang berwenang	6,6 mins	Wed 03/01/18	Wed 03/01/18	107	Teknisi Sarpras SI/TI
109.	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait pemeriksaan peralatan setelah dilakukan pemeliharaan	6,6 mins	Wed 03/01/18	Wed 03/01/18	108	Teknisi Sarpras SI/TI
110.	Auditor melakukan cek terhadap pencatatan pemeliharaan peralatan terkait pemeriksaan peralatan setelah dilakukan pemeliharaan	6,6 mins	Wed 03/01/18	Wed 03/01/18	109	Teknisi Sarpras SI/TI
111.	Auditor menanyakan kepada Teknisi srarpras SI/TIterkait penjadwalan pemeliharaan peralatan	6,6 mins	Wed 03/01/18	Wed 03/01/18	110	Teknisi Sarpras SI/TI
112.	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait ketersediaan kebijakan proses pemeliharaan yang dilakukan di tempat (ruang server)	6,6 mins	Wed 03/01/18	Wed 03/01/18	111	Teknisi Sarpras SI/TI
113.	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait pemeriksaan peralatan setelah dilakukan pemeliharaan	6,6 mins	Wed 03/01/18	Wed 03/01/18	112	Teknisi Sarpras SI/TI
114.	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait ketersediaan kebijakan pemeliharaan yang akan menggunakan jasa ekternal	6,6 mins	Wed 03/01/18	Wed 03/01/18	113	Teknisi Sarpras SI/TI
115.	Auditor menanyakan kepada Teknisi srarpras SI/TI terkait ketersediaan prosedur penghapusan informasi rahasia pada peralatan yang akan dilakukan pemeliharaan	6,6 mins	Wed 03/01/18	Wed 03/01/18	114	Teknisi Sarpras SI/TI
116.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait pengidentifikasian orang yang memiliki tanggung jawab memberikan izin peminjaman aset	6,6 mins	Wed 03/01/18	Wed 03/01/18	115	Teknisi Sarpras SI/TI
117.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya	6,6 mins	Wed	Wed	116	Teknisi Sarpras SI/TI

	prosedur peminjaman aset TI		03/01/18	03/01/18		
118.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya pencatatan peminjaman aset	6,6 mins	Wed 03/01/18	Wed 03/01/18	117	Teknisi Sarpras SI/TI
119.	Auditor melakukan cek terkait adanya proses verifikasi batas waktu peminjaman set dalam prosedur pemindahan aset	6,6 mins	Wed 03/01/18	Wed 03/01/18	118	Teknisi Sarpras SI/TI
120.	Auditor melakukan cek pada dokumen pencatatan peminjaman aset terkait adanya pencatatan barang ketika dikembalikan	6,6 mins	Wed 03/01/18	Wed 03/01/18	119	Teknisi Sarpras SI/TI
121.	Auditor melakukan cek pada pencatatan peminjaman aset terkait adanya informasi identitas, jabatan, dan tujuan	6,6 mins	Wed 03/01/18	Wed 03/01/18	120	Teknisi Sarpras SI/TI
122.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya kebijakan penggunaan peralatan diluar organisasi	6,6 mins	Wed 03/01/18	Wed 03/01/18	121	Teknisi Sarpras SI/TI
123.	Auditor menanykan kepada teknisi sarpras SI/TI terkait adanya pencatatan penggunaan peralan dan media diluar ruang server	6,6 mins	Wed 03/01/18	Wed 03/01/18	122	Teknisi Sarpras SI/TI
124.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya instruksi produsen mengenai pengaman peralatan yang dipakai diluar	6,6 mins	Wed 03/01/18	Wed 03/01/18	123	Teknisi Sarpras SI/TI
125.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait pengelolaan risiko terhadap penggunaan peralatan dan media diluar organisasi	6,6 mins	Wed 03/01/18	Wed 03/01/18	124	Teknisi Sarpras SI/TI
126.	Auditor menayakan kepada teknisi sarpras SI/TI terkait adanya prosedur pengalihan barang yang digunakan diluar ruang server	6,6 mins	Wed 03/01/18	Wed 03/01/18	125	Teknisi Sarpras SI/TI
127.	Auditor melakukan cek dokumen pencatatan terkait adanya pendefiniasn nama dan organisasi yang bertanggunng jawab pada peralatan	6,6 mins	Wed 03/01/18	Wed 03/01/18	126	Teknisi Sarpras SI/TI
128.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersedian prosedur penghapusan informasi pada media penyimpanan	6,6 mins	Wed 03/01/18	Wed 03/01/18	127	Teknisi Sarpras SI/TI
129.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya proses verifikasi sebelum dibuang atau digunakan kembali terhadap media penyimpanan	6,6 mins	Wed 03/01/18	Wed 03/01/18	128	Teknisi Sarpras SI/TI
130.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur yang mengatur teknik penghapusan dan penimpaan pada media penyimpanan	6,6 mins	Wed 03/01/18	Wed 03/01/18	129	Teknisi Sarpras SI/TI
131.	Auditor melakukan cek kesesuaian teknik penghapusan atau penimpaan yang digunakan oleh karyawan terhadap prosedur yang ada	6,6 mins	Wed 03/01/18	Wed 03/01/18	130	Teknisi Sarpras SI/TI
132.	Auditor menanyakan terkait ketersediaan prosedur perlindungan perlatan	6,6 mins	Wed	Wed	131	Teknisi Sarpras SI/TI

	yang tidak diawasi kepada teknis sarpras SI/TI		03/01/18	03/01/18		
133.	Auditor melakukan cek terhadap komputer teknis sarpras SI/TI terkait penggunaan password screean saver	6,6 mins	Wed 03/01/18	Wed 03/01/18	132	Teknisi Sarpras SI/TI
134.	Auditor melakukan cek terhadap komputer yang digunakan teknis sarpras SI/TI terkait log-off dari aplikasi atau layanan jaringan ketika tidak digunakan	6,6 mins	Wed 03/01/18	Wed 03/01/18	133	Teknisi Sarpras SI/TI
135.	Auditor melakukan cek terhadap computer atau handphone yang digunakan teknis sarpras SI/TI terkait ketersedian penggunaan password	6,6 mins	Wed 03/01/18	Wed 03/01/18	134	Teknisi Sarpras SI/TI
136.	Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur penyimpanan informasi bisnis yang kritis atau sensitive yang berupa dokumen kertas atau media penyimpanan elektronik kepada teknis sarpras SI/TI	6,6 mins	Wed 03/01/18	Wed 03/01/18	135	Teknisi Sarpras SI/TI
137.	Auditor melakukan cek ke dalam ruang server terkait ketersediaan lemeri penyimpanan dokumen yang berisi informasi kritis	6,6 mins	Wed 03/01/18	Wed 03/01/18	136	Teknisi Sarpras SI/TI
138.	Auditor melakukan cek terdahap keamanan lemari penyimpanan dokumen yang berisi informasi kritis	6,6 mins	Wed 03/01/18	Wed 03/01/18	137	Teknisi Sarpras SI/TI
139.	Auditor melakukan cek ke ruang server terkait ketersediaan media penyimpanan elektronik	6,6 mins	Wed 03/01/18	Wed 03/01/18	138	Teknisi Sarpras SI/TI
140.	Auditor menanyakan ketersediaan kepada sarpras SI/TI terkait prosedur penguncian komputer saat digunakaan	6,6 mins	Wed 03/01/18	Wed 03/01/18	139	Teknisi Sarpras SI/TI
141.	Auditor melakukan cek terhadap komputer yang digunakan teknisi sarpras SI/TI diruang server terkait penggunaan password pada komputer	6,6 mins	Wed 03/01/18	Wed 03/01/18	140	Teknisi Sarpras SI/TI
142.	Auditor melakukan cek ketersediaan kepada sarpras SI/TI terkait daftar pengguna peralatan seperti mesin fotokopi, scanner dan kamera digital di ruang server	6,6 mins	Wed 03/01/18	Wed 03/01/18	141	Teknisi Sarpras SI/TI
143.	Auditor menanyakan kepada sarpras SI/TI terkait ketersediaan peraturan yang melarang penggunaan peralatan seperti mesin fotokopi, scanner dan kamera di ruang server selain daftar pengguna	6,6 mins	Wed 03/01/18	Wed 03/01/18	142	Teknisi Sarpras SI/TI
144.	Auditor melakukan cek ketersediaan kebijakan penghapusan informasi sensitif atau rahasia dari printer	6,6 mins	Wed 03/01/18	Wed 03/01/18	143	Teknisi Sarpras SI/TI

LAMPIRAN C
VERIFIKASI DAFTAR CEK AUDIT

Tabel C.1 Verifikasi Dokumen Audit Program 1

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**	**Cek**
Control Objective	***Implementation Guidance***		
11.1.1 *Physical Security Perimeter*	a. perimeter (denah) keamanan harus didefinisikan, dan peletakan dan kekuatan dari masing-masing perimeter harus didasarkan pada kebutuhan keamanan aset dalam perimeter dan hasil penilaian risiko;	1. Auditor menanyakan kepada pengadministrasian BMN terkait adanya kebutuhan perimeter untuk melindungi aset 2. Auditor menanyakan kepada Pengadministrasian BMN terkait pendefinisian perimeter keamanan pada ruang server 3. Auditor melakukan cek ketersediaan pendefinisan letak dalam denah bangunan ruang server 4. Auditor melakukan cek ketersediaan pendefinisian konstruksi dalam denah	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
		bangunan ruang server 5. Auditor melakukan cek kesesuaian letak bangunan ruang server dengan denah bangunan ruang server 6. Auditor melakukan cek kesesuaian konstruksi bangunan dengan denah bangunan ruang server	
	b. bangunan atau tempat yang berisi fasilitas pengolahan informasi secara fisik harus kedap suara ; atap eksterior, dinding dan lantai dari bangunan harus dari konstruksi yang solid dan semua pintu eksternal harus dilindungi terhadap akses yang tidak sah sesuai dengan mekanisme kontrol, (misalnya alarm dan kunci); pintu dan jendela luar harus terkunci	7. Auditor melakukan cek terhadap bangunan terkait adanya celah pada bangunan 8. Auditor melakukan cek pada konstruksi atap, dinding dan lantai 9. Auditor melakukan cek pada pintu luar ruang server terkait adanya pengamanan akses masuk 10. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
	ketika ruangan ditinggalkan;	pengguncian pintu dan jendela eksternal ketika ditinggalkan	
	c. area resepsionis atau cara lain untuk mengendalikan akses fisik ke lokasi atau bangunan harus di tempat; akses ke tempat dan bangunan harus dibatasi hanya untuk orang untuk orang yang berwenang saja	11. Auditor melakukan cek terkait adanya area resepsionis 12. Auditor menanyakan kepada teknisi sarpras SI/TI terkait daftar orang yang boleh masuk keruang server	✓
	d. penghalang fisik harus, dibangun untuk mencegah akses fisik tidak sah dan pencemaran lingkungan;	13. Auditor melakukan cek terkait adanya batasan fisik dengan ruangan lain	✓
	e. semua pemicu kebakaran pada bangunan harus diperhitungkan, dipantau dan diuji; dalam membangun dinding harus didasarkan dengan standar regional, nasional dan	14. Auditor menanyakan kepada pengadministrasian BMN terkait adanya standar yang yang diacu dalam memilih konstruksi yang anti api 15. Auditor melakukan cek kesesuaian	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
	internasional yang sesuai;	konsruksi bangunan dengan standar yang diacu	
	f. Sistem pendeteksi penyusup yang cocok harus dipasang dan secara teratur diuji yang mencakup pintu dan jendela yang mungkin diakses; daerah kosong harus diamankan	16. Auditor memeriksa ketersediaan alat pendeteksi penyusup di ruang server 17. Auditor menanyakan kepada pengadministrasian BMN terkait adanya standar yang yang diacu dalam memilih alat pendeteksi 18. Auditor menanyakan kepada pengadministrasian BMN terkait adanya daftar spesifikasi alat pendeteksi 19. Auditor melakukan cek kesesuaian daftar spesifikasi alat pendeteksi penyusup dengan standar yang ada 20. Auditor melakukan cek ketersediaan ruang computer di ruang server	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
	i. Fasilitas pengolahan informasi yang dikelola oleh organisasi harus secara fisik dipisahkan dari yang dikelola oleh pihak eksternal	21. Auditor melakukan cek terkait pemisahan fasilitas pengolahan informasi secara fisik yang dikelola oleh organisasi dengan pihak eksternal	✓

Tabel C.2 Verifikasi Dokumen Audit Program 2

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**	**Cek**
Control Objective	***Implementation Guidance***		
11.1.2 Physical entry controls	a. 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. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersedian pencatatan pengunjung yang masuk ke ruang server 2. Auditor melakukan cek terhadap dokumen pencatatan terkait ketersedian penginformasian tanggal dan waktu masuk dan keluar pengunjung 3. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersedian prosedur pengawasan terhadap pengunjung	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
		4. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur akses masuk ke ruang server kepada teknis sarpras SI/TI 5. Auditor melakukan cek terhadap dokumen pecatatan pengunjung yang masuk terkait ketersediaan indentitas pengunjung yang masuk	
	b. 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 dua faktor seperti	6. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersesdiaan kontrol akses bagi orang yang memiliki kewenangan untuk masuk 7. Auditor melakukan cek	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
	kartu akses dan PIN rahasia	terhadap kontrol akses yang digunakan terkait penerapan otentikasi 2 faktor	
	c. Buku log fisik atau audit trail elektronik dari semua akses harus aman dijaga dan dipantau	8. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur pengelolaan log akses pengunjung yang berupa buku atau bersifat elektronik kepada teknis sarpras SI/TI 9. Auditor melakukan cek terhadap penyimpanan log akses yang berupa buku atau bersifat elektronik	✓
	d. Seluruh karyawan, kontraktor dan pihak eksternal harus diminta untuk memakai beberapa bentuk identifikasi terlihat dan	10. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur masuk	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
	harus segera memberitahukan petugas keamanan jika mereka menghadapi pengunjung tidak dikawal dan siapa pun yang tidak memakai identifikasi terlihat	ruang server semua karyawan, kontraktor, pihak external kepada teknis sarpras SI/TI 11. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan identitas pengenal bagi semua karyawan, kontraktor, dan pihak eksternal yang memiliki akses ke ruang server 12. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersedian prosedur pelaporan terkait pengunjung yang dikawal dan yang tidak disahkan aksesnya 13. Auditor menanyakan kepada	

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
		teknisi sarpras SI/TI terkait ketersedian prosedur pelaporan terkait pengunjung yang tidak memakai identitas pengenal	
	e. tenaga layanan pendukung dari pihak luar harus diberikan akses yang terbatas untuk mengamankan daerah atau fasilitas pengolahan informasi rahasia hanya ketika diperlukan; Akses ini harus disahkan dan dipantau;	14. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan daftar orang yang memiliki akses ke ruang server kepada teknis sarpras SI/TI 15. Auditor melakukan cek terhadap daftar orang yang memiliki akses ke ruang server terkait ketersedian hak akses bagi tenaga layanan pendukung dari luar 16. Auditor menanyakan kepada teknisi sarpras SI/TI terkait	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
		ketersediaan prosedur akses masuk bagi tenaga layanan pendukung dari luar	
	f. Hak akses untuk mengamankan area harus secara berkala dan diperbarui, dan dicabut bila diperlukan	17. Auditor melakukan cek terkait ketersediaan pembaharuan daftar hak askes bagi karyawan atau pihak ketiga yang telah putus kontrak 18. Auditor menanyakan kepada teknisi sarpras SI/TI ketersediaan daftar hak akses yang diperbaruai dan sebelum diperbarui	✓

Tabel C.3 Verifikasi Dokumen Audit Program 3

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**	**Cek**
Control Objective	***Implementation Guidance***		
11.1.1 *Physical Security Perimeter*	a. Fasilitas penting harus diletakkan untuk menghindari akses oleh publik	1. Auditor menanyakan kepada pengadministrasian BMN terkait aturan penentuan letak fasilitas seperti pintu dan jendela pada ruang server 2. Auditor melakukan cek kesesuaian letak pintu dan jendela dengan aturan penentuan letaknya	✓
	b. Jika dapat diaplikasikan, bangunan harus bebas dari gangguan dan memberikan indikasi minimal tujuan mereka, dengan tidak ada tanda-tanda yang jelas, di luar atau di dalam gedung, mengidentifikasi adanya kegiatan pengolahan informasi	3. Auditor melakukan cek terkait adanya tanda keberadaan ruang server	✓
	c. Fasilitas harus dikonfigurasi untuk mencegah informasi atau kegiatan	4. Auditor melakukan cek fasilitas ruang server yang dapat terdengar atau	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
	rahasia terlihat dan terdengar dari luar. Perisai elektromagnetik juga harus dipertimbangkan	terlihanya informasi atau kegiatan rahasia	
	d. Direktori dan buku telepon internal yang menyimpan lokasi dari fasilitas pengolahan informasi rahasia tidak boleh mudah diakses siapa pun yang tidak sah	5. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya direktori dan buku telepon internal 6. Auditor melakukan cek terhadap direktori dan buku telepon internal	✓

Tabel C.4 Verifikasi Dokumen Audit Program 4

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**	**Cek**
Control Objective	***Implementation Guidance***		
11.1.4 Protecting against external and environmental threats	a. Saran spesialis harus diperoleh tentang cara untuk menghindari kerusakan dari kebakaran, banjir, gempa bumi, ledakan, kerusuhan sipil dan bentuk lain dari bencana alam	1. Auditor menanyakan kepada pengadministrasian BMN terkait ketersediaan pendefinisian saran spesialis tentang memberikan pengamanan ruang server 2. Auditor melakukan cek terkait ketersediaan penentuan letak dalam dokumen saran spesialis 3. Auditor melakukan cek terhadap letak ruang server terkait kesesuaian dengan dokumen saran spesialis 4. Auditor melakukan cek terkait ketersediaan penentuan konstruksi bagunan yang harus digunakan dalam dokumen saran spesialis 5. Auditor melakukan cek terhadap	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
		konstruksi bangunan ruang server terkait kesesuaian dengan dokumen saran spesialis 6. Auditor melakukan cek terkait ketersediaan penentuan alat pendukung yang harus digunakan dalam dokumen saran spesialis 7. Auditor melakukan cek terhadap alat pendukung yang ada di ruang server terkait kesesuaian dengan dokumen saran spesialis	

Tabel C.5 Verifikasi Dokumen Audit Program 5

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**	**Cek**
Control Objective	***Implementation Guidance***		
11.1.5 Working in secure areas	a. Personel harus menyadari adanya, atau kegiatan dalam, daerah aman	1. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur kerja	✓
	b. Pekerjaan tanpa pengawasan di daerah aman harus dihindari baik untuk alasan keamanan dan untuk mencegah peluang untuk kegiatan berbahaya	2. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya peraturan yang melarang kerja tanpa pengawasan diruang server	✓
	c. Area aman yang kosong harus secara fisik terkunci dan secara periodic diperiksa	3. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur penguncian ruang server saat ditinggalkan 4. Auditor melakukan cek terkait adanya pengamanan pada pintu di ruang server	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
	d. Fotografi, video, audio atau peralatan rekaman lainnya, seperti kamera di perangkat mobile, seharusnya tidak diperbolehkan, kecuali diizinkan	5. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya peraturan yang melarang kegiatan merekam	✓

Tabel C.6 Verifikasi Dokumen Audit Program 6

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**	**Cek**
Control Objective	***Implementation Guidance***		
11.1.6 Delivery and loading areas	a. Akses ke wilayah pengiriman dan penerimaan dari luar gedung harus dibatasi hanya untuk personel yang berwenang;	1. Auditor melakukan cek terkait adanya area pengiriman dan penerimaan barang di sekitar ruang server. 2. Auditor menanyakan kepada teknisi sarpras SI/TI terkait pengidentifikasiaan personel yang bertanggung jawab mengawasi di area pengiriman dan penerimaan barang	✓
	b. Wilayah pengiriman dan pemuatan daerah harus dirancang agar pasokan dapat dimuat dan dibongkar tanpa personil pengiriman mendapatkan akses ke bagian lain dari bangunan	3. Auditor menanyakan kepada pengadministrasian BMN terkait adanya desing bangunan dan letak area pengiriman dan penerimaan barang 4. Auditor melakukan cek area pengiriman dan penerimaan barang terkait kesesuaian dengan design yang dibuat	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
	c. Pintu eksternal dari pengiriman dan pemuatan daerah harus diamankan ketika pintu internal dibuka	5. Auditor melakukan cek terhadap area pengiriman dan penerimaan barang terkait keamanan akses ke gedung lain	✓
	d. Bahan yang masuk harus diperiksa dan diperiksa untuk bahan peledak, bahan kimia atau bahan berbahaya lainnya, sebelum pindah dari wilayah pengiriman dan pemuatan	6. Auditor menanyakan kepada pengadministrasian BMN terkait adanya prosedur pemeriksaan barang 7. Auditor melakukann cek terkait adanya pencatatan pemeriksaan barang	✓
	e. Bahan yang masuk harus didaftarkan sesuai dengan prosedur manajemen aset saat masuk ke area kerja	8. Auditor menanyakan kepada pengadministrasian BMN terkait adanya prosedur manajemen aset 9. Auditor melakukann cek terkait adanya pencatatan barang yang masuk ke area kerja	✓
	f. Pengiriman masuk dan keluar harus	10. Auditor melakukan cek terkait	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
	secara fisik terpisah, jika dimungkinkan	pemisahan ruang pengiriman dengan ruang penerimaan barang	
	g. Bahan yang masuk harus diperiksa untuk bukti gangguan perjalanan. Jika gangguan tersebut ditemukan harus segera dilaporkan kepada petugas keamanan	11. Auditor melakukan cek terhadap prosedur pemeriksaan barang terkait adanya pemeriksaan barang yang mengalami gangguan 12. Auditor menanyakan kepada pengadministrasian BMN terkait adanya prosedur pelaporan barang yang mengalami gangguan pengiriman	✓

Tabel C.7 Verifikasi Dokumen Audit Program 7

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**	**Cek**
Control Objective	***Implementation Guidance***		
11.2.1 Equipment siting and protection	a. Peralatan harus diletakkan untuk meminimalkan akses yang tidak perlu ke daerah kerja	1. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan ketentuan peletakan peralatan 2. Auditor melakukan cek terkait kesesuaian penempatan peralatan yang ada dengan dokumen ketentuan peletakan peralatan	✓
	b. Fasilitas pengolahan informasi yang menangani data sensitif harus diposisikan hati-hati untuk mengurangi risiko informasi dilihat oleh orang yang tidak berwenang selama penggunaannya	3. Auditor melakukan cek terhadap fasilitas pengolahan informasi yang menangangi data sensitif terkait kesesuaian terhadap dokumen ketentuan peletakan	✓
	c. Fasilitas penyimpanan harus diamankan untuk menghindari akses yang tidak sah	4. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur pengamanan fasilitas	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
		penyimpanan 5. Auditor melakukan cek terkait keamanan pada fasilitas penyimpanan	
	d. Barang yang membutuhkan perlindungan khusus harus dijaga untuk mengurangi tingkat umum perlindungan yang diperlukan	6. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan daftar peralatan yang membutuhkan pengamanan khusus 7. Auditor melakukan cek terkait ketersediaan kebutuhan pengamanan yang ada pada daftar peralatan yang membutuhkan pengamanan khusus 8. Auditor melakukan cek terkait kesesuaian pengamanan yang ada pada peralatan yang membutuhkan pengamanan khusus terhadap	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
		kebutuhan yang ditentukan	
	e. Kontrol harus diadopsi untuk meminimalkan risiko potensial ancaman fisik dan lingkungan, misalnya pencurian, kebakaran, bahan peledak, asap, air (atau kegagalan pasokan air), debu, getaran, efek kimia, gangguan pasokan listrik, gangguan komunikasi, radiasi elektromagnetik dan vandalisme	9. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan pengelolaan risiko yang ada diruang server terkait risiko ancaman fisik dan lingkungan 10. Auditor melakukan cek terkait kesesuaian control yang di adopsi pada dokumen pengelolaan risiko terkait risiko ancaman fisik dan lingkungan	✓
	f. Pedoman untuk makan, minum dan merokok di dekat fasilitas pengolahan informasi harus ditetapkan	11. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan prosedur mengenai makan, minum dan merokok didekat fasilitas pengolahan informasi	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
	g. Kondisi lingkungan, seperti suhu dan kelembaban, harus dipantau untuk kondisi yang dapat mempengaruhi pengoperasian fasilitas pengolahan informasi	12. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan ketentuan suhu di ruang server 13. Auditor melakukan cek kesesuaian suhu dalam ruang server terhadap ketentuuan yang ada	✓
	h. Perlindungan dari petir harus diterapkan untuk semua bangunan dan filter proteksi petir harus dipasang untuk semua kekuatan yang masuk dan jalur komunikasi	14. Auditor melakukan cek ketersediaan penangkal petir pada bangunan ruang server 15. Auditor melakukann cek ketersediaan pelindung elektromagnetik pada peralatan pengolahan informasi rahasia	✓

Tabel C.8 Verifikasi Dokumen Audit Program 8

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**	**Cek**
Control Objective	***Implementation Guidance***		
11.1.1 *Physical Security Perimeter*	a. Penyesuaian dengan spesifikasi peralatan pabrik dan persyaratan hukum lokal	1. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan kebutuhan peralatan pendukung di IS-net 2. Auditor melakukan cek kesesuaian peralatan pendukung yang ada dengan daftar kebutuhan peralatan pendukung	✓
	b. Penilaian secara teratur untuk kapasitas mereka untuk memenuhi pertumbuhan bisnis dan interaksi dengan utilitas pendukung lainnya	3. Auditor menanyakan kepada teknis sarpras listrik terkait ketersediaan kebijakan untuk melakukan penilaian kapasitas peralatan yang ada terhadap pemenuhan pertumbuhan bisnis dan interaksi dengan peralatan pendukung lainnya 4. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersediaan penilaian kapasitas peralatan	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
	c. Pemeriksaan dan pengujian secara teratur untuk memastikan fungsi yang tepat	5. Auditor menanyakan kepada teknis sarpras listrik terkait adanya pemeriksaan dan pengujian peralatan pendukung untuk memastikan dapat berfungsi dengan baik 6. Auditor melakukan cek terhadap dokumen pemeriksaan dan pengujian peralatan pendukung terkait kapan dilakukannya pemeriksaan dan pengujian	✓
	d. Jika perlu, beri alarm untuk mendeteksi malfungsi	7. Auditor melakkukan cek terhadap peralatan pendukung terkait adanya pendeteksi malfungsi	✓
	e. Jika perlu, miliki beberapa feed routing fisik yang beragam	8. Auditor menanyakan kepada teknisi sarpras listrik terkait ketersediaan kebijakan penggunaan lebih dari 1 sumber setiap peralatan pendukung	✓

Tabel C.9 Verifikasi Dokumen Audit Program 9

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
11.2.3 Cabling security	a. Kabel daya dan telekomunikasi ke fasilitas pengolahan informasi harus di bawah tanah, jika memungkinkan, berikan perlindungan alternatif yang memadai	1. Auditor melakukan cek pada instalasi kabel listrik dan kabel telekomunikasi terkait penempatan kabel 2. Auditor melakukan cek terkait adanya perlindungan alternative pada kabel kepada teknis srpras listrik	✓
	b. Kabel listrik harus dipisahkan dari kabel komunikasi untuk mencegah gangguan	3. Auditor melakukan cek terhadap kabel telekomunikasi dan kabel listrik terkait pemisahan jalur kabel	✓
	c. Untuk sistem sensitif atau kritis lanjut kontrol untuk dipertimbangkan termasuk: 1) instalasi saluran lapis baja dan mengunci ruangan atau kotak pada titik	4. Auditor menyakan kepada teknisi sarpras listrik terkait ketersediaan himbauan instalasi saluran lapis baja 5. Auditor melakukan cek terhadap	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
	pemeriksaan dan pemutusan; 2) menggunakan pelindung elektromagnetik untuk melindungi kabel; 3) inisiasi peembersihan teknis dan pemeriksaan fisik untuk perangkat yang tidak sah yang melekat pada kabel; 4) akses dikendalikan untuk patch panel dan ruang kabel.	kabel yang menyambung pada server terkait instalasi saluran lapis baja 6. Auditor menanyakan kepada teknisi sarpras listrik terkait adanya himbauan penguncian kotak inspeksi dan pemutusan listrik 7. Auditor menanyakan kepada teknisi sarpras listrik terkait adanya himbauan instalasi kabel dengan penggunaan pelindung elektromagnetik 8. Auditor melakukan cek terhadap kabel yang menyambung pada server terkait penggunaan pelindung elektromagnetik 9. Auditor menayakan kepada teknisi	

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
		sarpras listrik terkait ketersedian prosedur pengendalian akses ke patch panel dan ruangan kabel 10. Auditor melakukan cek ke patch panel dan ruangan kabel terkait adanya penguncian patch panel atau ruangan kabel	

Tabel C.10 Verifikasi Dokumen Audit Program 10

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**	**Cek**
Control Objective	***Implementation Guidance***		
11.2.4 Equipment maintenance	a. Peralatan harus dipelihara sesuai dengan interval servis pemasok yang dianjurkan dan spesifikasi	1. Auditor menayakan kepada Teknisi srarpras SI/TI terkait adanya anjuran pemeliharan peralatan dari pemasok 2. Auditor menanyakan kepada srarpras SI/TI terkait ketersediaan pencatatan pemeliharaan peralatan 3. Auditor menanyakan kepada Teknisi srarpras SI/TI terkait adanya pencatatan pemeliharaan peralatan yang dianjurkan oleh pemasok	✓
	b. Semua kebutuhan perawatan yang dianjurkan oleh kebijakan asuransi harus dipenuhi	4. Auditor menanyakan kepada srarpras SI/TI terkait adanya kebijakan asuransi mengenai	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
		kebutuhan pemeliharaan peralatan 5. Auditor menanyakan kepada Teknisi srarpras SI/TI terkait adanya pencatatan pemeliharaan peralatan yang dianjurkan oleh pihak asuransi	
	c. Hanya personil pemeliharaan yang berwenang yang harus melakukan perbaikan dan layanan peralatan	6. Auditor menanyakan kepada srarpras SI/TI terkait kewenangan proses pemeliharaan peralatan 7. Auditor melakukan cek terhadap pencatatan pemeliharaan peralatan terkait orang yang berwenang	✓
	d. Catatan perkiraan kesalahan atau	8. Auditor menanyakan kepada	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
	kesalahan aktual, dan semua pemeliharaan preventif dan korektif harus disimpan	srarpras SI/TI terkait pemeriksaan peralatan setelah dilakukan pemeliharaan 9. Auditor melakukan cek terhadap pencatatan pemeliharaan peralatan terkait pemeriksaan peralatan setelah dilakukan pemeliharaan	
	e. Pengendalian yang tepat harus dilaksanakan bila peralatan dijadwalkan untuk pemeliharaan, dengan mempertimbangkan apakah perawatan ini dilakukan oleh personel	10. Auditor menanyakan kepada srarpras SI/TI terkait penjadwalan pemeliharaan peralatan 11. Auditor menanyakan kepada srarpras SI/TI terkait ketersediaan kebijakan proses pemeliharaan yang dilakukan di	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
		tempat (ruang server) 12. Auditor menanyakan kepada srarpras SI/TI terkait ketersediaan kebijakan pemeliharaan yang akan menggunakan jasa ekternal 13. Auditor menanyakan kepada srarpras SI/TI terkait ketersediaan prosedur penghapusan informasi rahasia pada peralatan yang akan dilakukan pemeliharaan	

Tabel C.11 Verifikasi Dokumen Audit Program 11

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**	**Cek**
Control Objective	***Implementation Guidance***		
11.1.1 *Physical Security Perimeter*	a. Karyawan dan pihak eksternal yang memiliki otoritas untuk mengizinkan peminjaman aset harus diidentifikasi	1. Auditor menanyakan kepada teknisi sarpras SI/TI terkait pengidentifikasian orang yang memiliki tanggung jawab memberikan izin peminjaman aset	✓
	b. Batas waktu peminjaman aset harus ditetapkan dan kembali diverifikasi untuk kepatuhan	2. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur peminjaman aset TI 3. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya pencatatan peminjaman aset 4. Auditor melakukan cek terkait adanya proses verifikasi batas waktu peminjaman set dalam prosedur peminjaman aset 5. Auditor melakukan cek pada	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
		pencatatan peminjaman aset terkait adanya checklist verifikasi	
	c. Bila perlu, aset harus dicatat sebagai aset yang dipinjam dan dicatat ketika kembali	6. Auditor melakukan cek pada dokumen pencatatan peminjaman aset terkait adanya pencatatan barang ketika dikembalikan	✓
	d. Identitas, peran dan afiliasi dari siapa saja yang menangani atau menggunakan aset harus didokumentasikan dan dokumentasi ini kembali dengan peralatan, informasi atau perangkat lunak	7. Auditor melakukan cek pada pencatatan peminjaman aset terkait adanya informasi identitas, jabatan, dan tujuan	✓

Tabel C.12 Verifikasi Dokumen Audit Program 12

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**	**Cek**
Control Objective	***Implementation Guidance***		
11.2.6 Security of equipment and assets off-premises	a. Peralatan dan media diambil dari tempat tidak boleh dibiarkan tanpa pengawasan di tempat umum	1. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya kebijakan penggunaan peralatan diluar organisasi 2. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya pencatatan penggunaan peralan dan media diluar ruang server	✓
	b. Instruksi produsen untuk melindungi peralatan harus diamati setiap saat, misalnya perlindungan terhadap paparan medan elektromagnetik yang kuat	3. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya instruksi produsen mengenai pengamanan peralatan yang dipakai diluar	✓
	c. Kontrol untuk lokasi *off-site*, seperti rumah kerja, teleworking dan situs sementara harus ditentukan oleh penilaian risiko dan control cocok	4. Auditor menanyakan kepada teknisi sarpras SI/TI terkait pengelolaan risiko terhadap penggunaan peralatan dan media diluar organisasi	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
	diterapkan sebagaimana mestinya, misalnya lemari arsip dikunci, kebijakan meja yang jelas, kontrol akses untuk komputer dan komunikasi yang aman dengan kantor		
	d. Ketika peralatan *off-site* ditransfer antara individu-individu yang berbeda atau pihak eksternal, log harus dipertahankan yang mendefinisikan lacak balak pada peralatan termasuk setidaknya nama dan organisasi dari orang-orang yang bertanggung jawab untuk peralatan	5. Auditor menayakan kepada teknisi sarpras SI/TI terkait adanya prosedur pengalihan peralatan yang digunakan diluar ruang server 6. Auditor melakukan cek dokumen pencatatan terkait adanya pendefiniasn nama dan organisasi yang bertanggunng jawab pada peralatan	✓

Tabel C.13 Verifikasi Dokumen Audit Program 13

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**	**Cek**
Control Objective	***Implementation Guidance***		
11.2.7 Secure disposal or re-use of equipment	a. Peralatan harus diverifikasi untuk memastikan apakah media penyimpanan yang terkandung sebelum dibuang atau digunakan kembali.	1. Auditor menanyakan kepada teknisi sarpras SI/TI terkait ketersedian prosedur penghapusan informasi pada media penyimpanan 2. Auditor melakukan cek terkait adanya proses verifikasi sebelum dibuang atau digunakan kembali terhadap media penyimpanan	✓

	b. Media penyimpanan yang berisi informasi rahasia atau hak cipta harus secara fisik dihancurkan atau informasinya harus dihancurkan, dihapus atau ditimpa menggunakan teknik untuk membuat informasi asli tidak dapat diambil kemabali daripada menggunakan standar menghapus atau fungsi Format	3. Auditor menanyakan kepada teknisi sarpras SI/TI terkait adanya prosedur yang mengatur teknik penghapusan dan penimpaan pada media penyimpanan 4. Auditor melakukan cek kesesuaian teknik penghapusan atau penimpaan yang digunakan oleh karyawan terhadap prosedur yang ada	✓

Tabel C.14 Verifikasi Dokumen Audit Program 14

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**	**Cek**
Control Objective	***Implementation Guidance***		
11.2.8 Unattended user equipment	a. Mengakhiri sesi aktif ketika selesai, kecuali bisa diamankan oleh mekanisme penguncian yang tepat, misalnya dilindungi password screen saver	1. Auditor menanyakan kepada teknis sarpras SI/TI terkait ketersediaan prosedur perlindungan perlatan yang tidak diawasi 2. Auditor melakukan cek terhadap komputer teknis sarpras SI/TI terkait penggunaan password screean saver	✓
	b. Log-off dari aplikasi atau layanan jaringan ketika tidak lagi dibutuhkan	3. Auditor melakukan cek terhadap komputer yang digunakan teknis sarpras SI/TI terkait log-off dari aplikasi atau layanan jaringan ketika tidak digunakan	✓
	c. Mengamankan komputer atau perangkat mobile dari penggunaan yang tidak sah	4. Auditor melakukan cek terhadap computer atau handphone yang	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
	oleh kunci kunci atau kontrol yang setara, misalnya akses password, jika tidak digunakan	digunakan teknis sarpras SI/TI terkait ketersedian penggunaan password	

Tabel C.15 Verifikasi Dokumen Audit Program 15

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		**Aktifitas Audit**	**Cek**
Control Objective	***Implementation Guidance***		
11.2.9 Clear desk and clear screen policy	a. Informasi bisnis yang sensitif atau kritis, misalnya di atas kertas atau media penyimpanan elektronik, harus terkunci (idealnya dalam bentuk yang aman atau lemari atau lainnya furnitur keamanan) bila tidak diperlukan, terutama ketika kantor dikosongkan.	1. Auditor menanyakan kepada teknis sarpras SI/TI terkait ketersediaan prosedur penyimpanan informasi bisnis yang kritis atau sensitive yang berupa dokumen kertas atau media penyimpanan elektronik 2. Auditor melakukan cek ke dalam ruang server terkait ketersediaan lemari penyimpanan dokumen yang berisi informasi kritis 3. Auditor melakukan cek terdahap keamanan lemari penyimpanan dokumen yang berisi informasi kritis	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
		4. Auditor melakukan cek ke ruang server terkait ketersediaan pengaman pada media penyimpanan elektronik	
	b. Komputer dan terminal harus dibiarkan log off atau dilindungi dengan layar dan keyboard dengan penguncian password, mekanisme otentikasi pengguna tanda atau serupa ketika tanpa pengawasan dan harus dilindungi oleh kunci kunci, password atau kontrol lain jika tidak digunakan	5. Auditor melakukan cek ketersediaan prosedur penguncian komputer saat tidak digunakaan 6. Auditor melakukan cek terhadap komputer yang digunakan teknisi sarpras SI/TI diruang server terkait penggunaan password pada computer	✓
	c. Penggunaan yang tidak sah dari mesin fotokopi dan teknologi reproduksi lainnya	7. Auditor menanyakan kepada teknisi sarpras SI/TI terkait	✓

ISO/IEC 27002:2013 Klausul 11 Keamanan Fisik dan Lingkungan		Aktifitas Audit	Cek
Control Objective	***Implementation Guidance***		
	(misalnya scanner, kamera digital) harus dicegah	ketersediaan daftar pengguna peralatan seperti mesin fotokopi, scanner dan kamera digital di ruang server 8. Auditor menanyakan kepada teknisi sarpras SI/TI ketersediaan peraturan yang melarang penggunaan peralatan seperti mesin fotokopi, scanner dan kamera di ruang server selain daftar pengguna	
	d. media yang mengandung informasi sensitif atau rahasia harus dihapus dari printer segera.	9. Auditor menanyakan kepada teknisi sarpras SI/TI kebijakan penghapusan informasi sensitif atau rahasia dari printer	✓

LAMPIRAN D
CONTOH PENGISIAN

PERANGKAT AUDIT KEAMANAN FISIK DAN LINGKUNGAN
TEKNOLOGI INFORMASI DI RUANG SERVER
JURUSAN SISTEM INFORMASI ITS (IS-NET)

Auditor:	*2. Equipment Security*	
	2.3 Cabling Security	
Tanggal Audit : dd mm yy	Kontrol : Kabel listrik dan telekomunikasi yang membawa data atau mendukung layanan informasi pendukung harus dilindungi dari intersepsi atau kerusakan.	

No.	Prosedur Audit	Daftar Cek Audit	Test	Iya	Tidak	Partial	Bukti
P.2.3.1	Auditor memeriksa instalasi kabel listrik dan kabel telekomunikasi	a. Apakah terdapat dokumen prosedur terkait instalasi kabel di ruang server?	Compliance	✓			*tersedia dokumen prosedur instalasi kabel*
		Temuan:					
		b. Periksa apakah semua kabel listrik dan kabel telekomunikasi telah berada di bawah lantai?	Substantive	✓			*Semua kabel listrik dan kabel telekomunikasi berada dibawah lantai* (Foto Kabel listrik dan kabel telekomunikasi yang berada dibawah lantai)
		Temuan:					
		c. Periksa apakah instalasi kabel listrik dan kabel telekomunikasi telah dipisahkan untuk mencegah terjadinya gangguan?	Substantive		✓		*Kabel istrik dan kabel telekomunikasi tidak dipisahkan* (Foto Kabel listrik dan kabel telekomunikasi)
		Temuan: *pada saat penginstalasian kabel, Kabel listrik dan kabel telekomunikasi tidak dipisahkan*					
P.2.3.2	Auditor memeriksa perlindungan instalasi saluran kabel daya dan	a. Periksa apakah kabel listrik dan kabel telekomunikasi telah dilindungi dengan pelapis baja?	Substantive			✓	*Hanya sebagian kabel yang dilindungi pelapis*

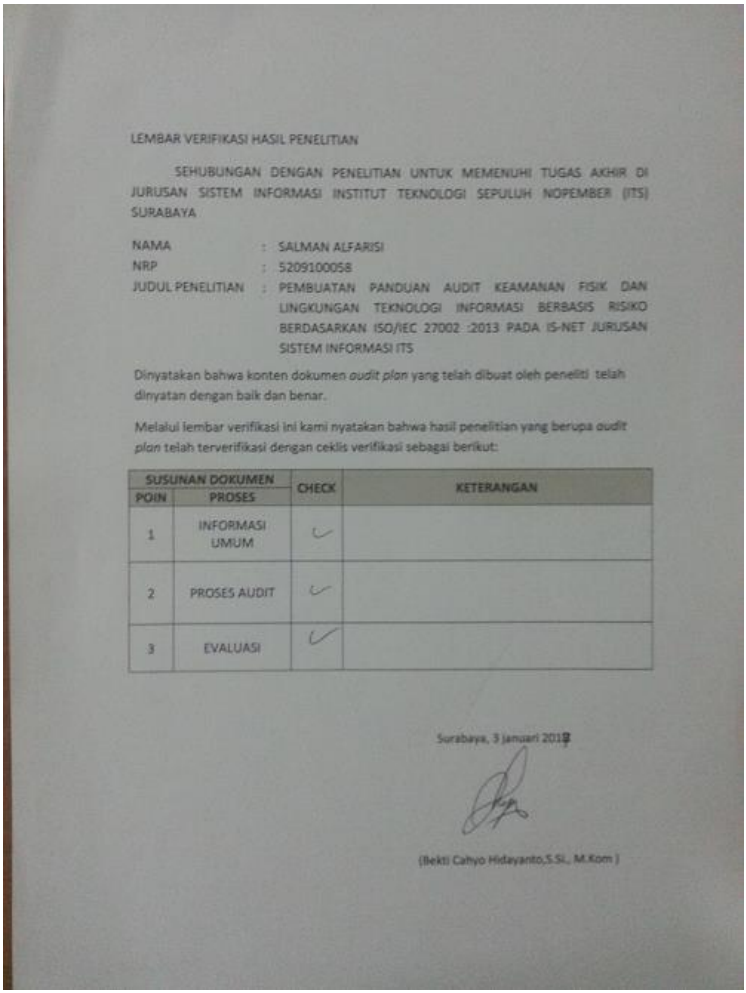
	kabel telekomunikasi	Temuan: *pada penginstalasian kabel Hanya kabel listrik yang dilindungi pelapis baja sementara kabel telekomunikasi tidak*					*baja* (foto kabel listrik dan kabel telekomunikasi)
		b. Periksa apakah ruangan atau kotak pada pusat pengawasan dan pemutusan kabel telah terkunci? (lakukan pemeriksaan dengan cara membukannya)	Substantive	✓			*ruangan atau kotak pada pusat pengawasan dan pemutusan kabel dalam posisi terkunci* (foto ruangan atau kotak pada pusat pengawasan dan pemutusan kabel dalam posisi terkunci)
		Temuan:					
		c. Periksa Apakah dalam instalasi kabel listrik dan telekomunikasi menggunakan pelindung elektromagnetik sebagai pelindung kabel?	Substantive		✓		*Kabel listrik dan kabel tidak menggunakan pelindung elektromagnetik* (foto kabel listrik dan telekomunikasi yang tidak memakai pelindung elektromagnetik)
		Temuan: *instalsi kabel listrik dan kabel telekomunikasi tidak menggunakan pelindung elektromagnetik*					
		d. Periksa apakah tidak terdapat perangkat yang tidak sah (unauthorized) yang melekat pada kabel? (lakukan pemeriksaan secara langsung pada jalur kabel listrik dan telekomunikasi)	Substantive	✓			*Tidak ada perangkat yang tidak sah yang melekat pada kabel* (foto perangkat yang tidak sah tidak ada yang melekat pada kabel)
		Temuan:					

		e. Apakah patch panel dan ruangan kabel memiliki pengamanan yang baik? (Lakukan pengamatan secara lansung apakah terdapat pengaman seperti kunci atau gembok pada pintu patch panel dan ruang kabel)	Substantive	✓			*Terdapat pengaman yang baik pada patch panel dan ruang kabel* (Foto pintu patch panel dan ruangan kabel memiliki kunci dan gembok)
		Temuan:					
		f. Apakah terdapat pencatatan akses masuk ke patch panel dan ruang kabel?			✓		*tidak ada pencatatan akses masuk ke patch panel dan ruang kabel* (tidak ada form akses masuk ke patch panel dan ruang kabel)
		Temuan: *tidak ada pencatatan akses masuk ke patch panel dan ruang kabel*					
		g. Apakah terdapat pelebelan pada kabel yang dikendalikan di *Cable Rooms*?	Compliance	✓			*Kabel yang ada pada ruang kabel diberi lebel* (foto kabel yang ada pada *Cable rooms*)
		Temuan:					

Gambar D.1 Contoh Pengisian Perangkat Audit

Halaman ini sengaja dikosongkan

LAMPIRAN E
HASIL VERIFIKASI PANDUAN AUDIT



LEMBAR VERIFIKASI HASIL PENELITIAN

SEHUBUNGAN DENGAN PENELITIAN UNTUK MEMENUHI TUGAS AKHIR DI JURUSAN SISTEM INFORMASI INSTITUT TEKNOLOGI SEPULUH NOPEMBER (ITS) SURABAYA

NAMA : SALMAN ALFARISI
NRP : 5209100058
JUDUL PENELITIAN : PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO/IEC 27002 :2013 PADA IS-NET JURUSAN SISTEM INFORMASI ITS

Dinyatakan bahwa konten dokumen *audit plan* yang telah dibuat oleh peneliti telah dinyatan dengan baik dan benar.

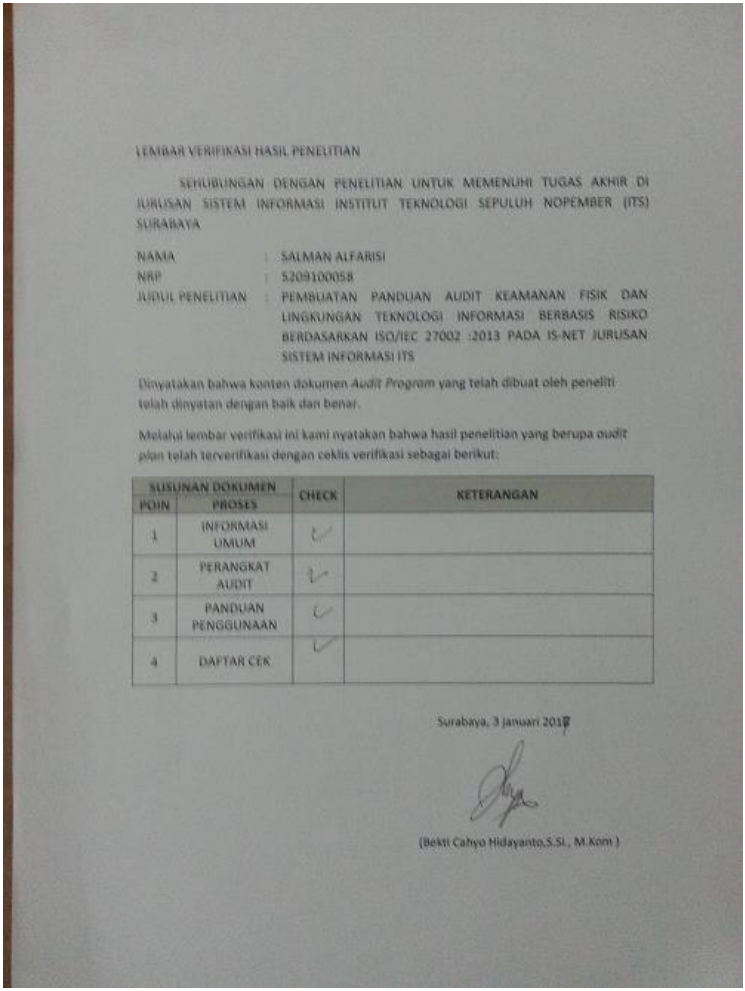
Melalui lembar verifikasi ini kami nyatakan bahwa hasil penelitian yang berupa *audit plan* telah terverifikasi dengan ceklis verifikasi sebagai berikut:

SUSUNAN DOKUMEN		CHECK	KETERANGAN
POIN	PROSES		
1	INFORMASI UMUM	✓	
2	PROSES AUDIT	✓	
3	EVALUASI	✓	

Surabaya, 3 januari 2018

(Bekti Cahyo Hidayanto,S.Si., M.Kom)

Gambar E.1 Verifikasi Audit Plan Oleh Pihak IS-Net



LEMBAR VERIFIKASI HASIL PENELITIAN

SEHUBUNGAN DENGAN PENELITIAN UNTUK MEMENUHI TUGAS AKHIR DI JURUSAN SISTEM INFORMASI INSTITUT TEKNOLOGI SEPULUH NOPEMBER (ITS) SURABAYA

NAMA : SALMAN ALFARISI
NRP : 5209100058
JUDUL PENELITIAN : PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO/IEC 27002 :2013 PADA IS-NET JURUSAN SISTEM INFORMASI ITS

Dinyatakan bahwa konten dokumen *Audit Program* yang telah dibuat oleh peneliti telah dinyatan dengan baik dan benar.

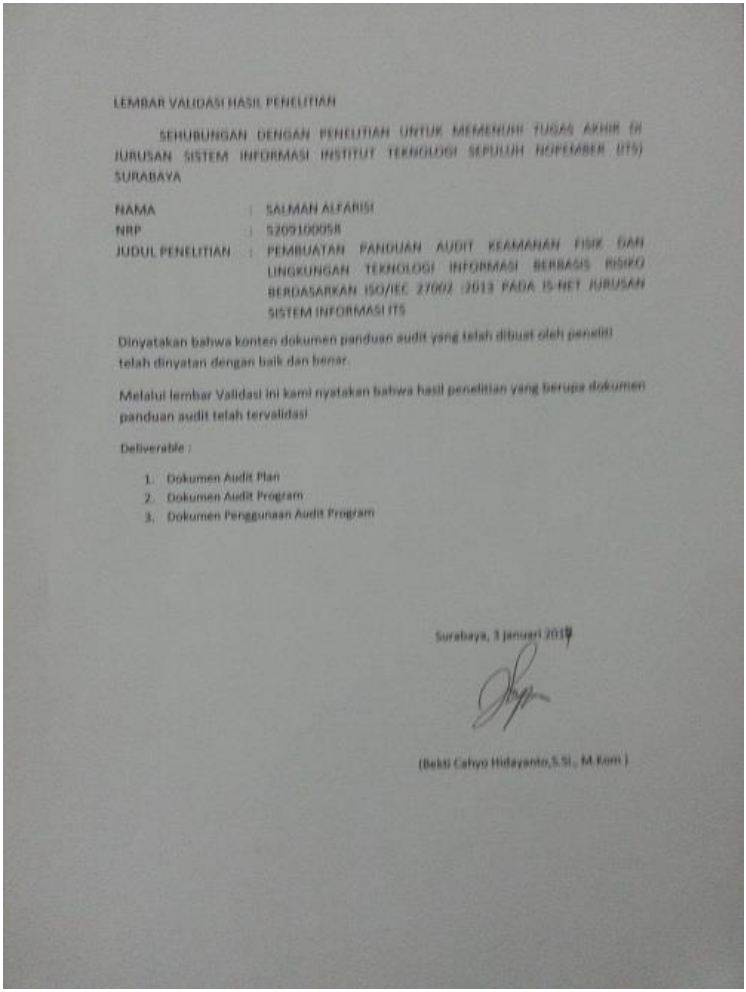
Melalui lembar verifikasi ini kami nyatakan bahwa hasil penelitian yang berupa audit plan telah terverifikasi dengan ceklis verifikasi sebagai berikut:

SUSUNAN DOKUMEN		CHECK	KETERANGAN
POIN	PROSES		
1	INFORMASI UMUM	✓	
2	PERANGKAT AUDIT	✓	
3	PANDUAN PENGGUNAAN	✓	
4	DAFTAR CEK	✓	

Surabaya, 3 Januari 2018

(Bekti Cahyo Hidayanto,S.SI., M.Kom)

Gambar E.2 Verifikasi Audit Program Oleh pihak IS-NET



LEMBAR VALIDASI HASIL PENELITIAN

SEHUBUNGAN DENGAN PENELITIAN UNTUK MEMENUHI TUGAS AKHIR DI JURUSAN SISTEM INFORMASI INSTITUT TEKNOLOGI SEPULUH NOPEMBER (ITS) SURABAYA

NAMA	:	SALMAN ALFARISI
NRP	:	5209100058
JUDUL PENELITIAN	:	PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO/IEC 27002 :2013 PADA IS-NET JURUSAN SISTEM INFORMASI ITS

Dinyatakan bahwa konten dokumen panduan audit yang telah dibuat oleh peneliti telah dinyatan dengan baik dan benar.

Melalui lembar Validasi ini kami nyatakan bahwa hasil penelitian yang berupa dokumen panduan audit telah tervalidasi

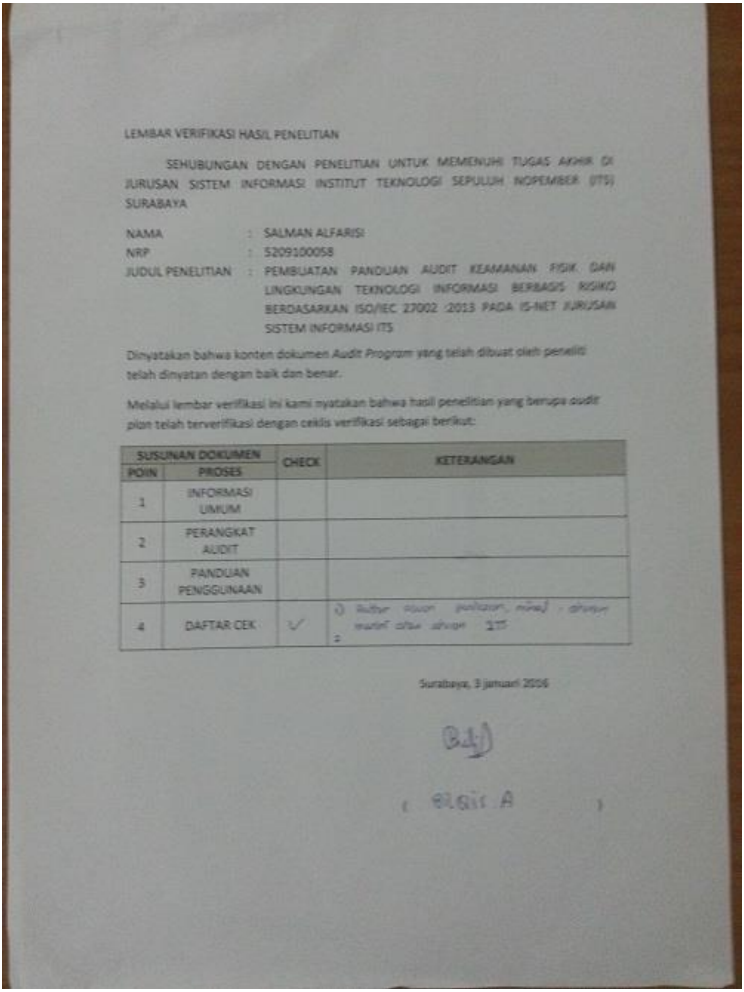
Deliverable :

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

Surabaya, 3 januari 2017

(Bekti Cahyo Hidayanto,S.Si., M.Kom)

Gamabar E.3 Validasi Panduan Audit Oleh Pihak IS-Net



LEMBAR VERIFIKASI HASIL PENELITIAN

SEHUBUNGAN DENGAN PENELITIAN UNTUK MEMENUHI TUGAS AKHIR DI JURUSAN SISTEM INFORMASI INSTITUT TEKNOLOGI SEPULUH NOPEMBER (ITS) SURABAYA

NAMA : SALMAN ALFARISI
NRP : 5209100058
JUDUL PENELITIAN : PEMBUATAN PANDUAN AUDIT KEAMANAN FISIK DAN LINGKUNGAN TEKNOLOGI INFORMASI BERBASIS RISIKO BERDASARKAN ISO/IEC 27002 :2013 PADA IS-NET JURUSAN SISTEM INFORMASI ITS

Dinyatakan bahwa konten dokumen *Audit Program* yang telah dibuat oleh peneliti telah dinyatan dengan baik dan benar.

Melalui lembar verifikasi ini kami nyatakan bahwa hasil penelitian yang berupa audit plan telah terverifikasi dengan ceklis verifikasi sebagai berikut:

SUSUNAN DOKUMEN		CHECK	KETERANGAN
POIN	PROSES		
1	INFORMASI UMUM		
2	PERANGKAT AUDIT		
3	PANDUAN PENGGUNAAN		
4	DAFTAR CEK	✓	1) [illegible] 2)

Surabaya, 3 januari 2016

(Bilqis A)

Gambar E.4 Verifikasi Audit Program Oleh pihak Auditor