TESIS - IS185401

PENYUSUNAN KEBIJAKAN KEAMANAN INFORMASI DENGAN PENILAIAN RISIKO KEAMANAN ASET PADA KAMPUS INSTITUT TEKNOLOGI SEPULUH NOPEMBER BERDASAR STANDAR ISO 27001

MURDIONO
05211650010027

Dosen Pembimbing
Dr.Eng. Febriliyan Samopa, S.Kom., M.Kom.
NIP: 197302191998021001

Departemen Sistem Informasi
Fakultas Teknologi Elektro Dan Informatika Cerdas
Institut Teknologi Sepuluh Nopember

2020

[Halaman ini sengaja dikosongkan]

TESIS - IS185401

INFORMATION SECURITY POLICY DEVELOPMENT USING ASSET RISK ASSESSMENT AT SEPULUH NOPEMBER INSTITUTE OF TECHNOLOGY BASED ON ISO 27001 STANDARDS

MURDIONO
05211650010027

Supervisor
Dr.Eng. Febriliyan Samopa, S.Kom., M.Kom.
NIP: 197302191998021001

Departement of Information System
Faculty Of Intelligent Electrical And Informatics Technology
Institut Teknologi Sepuluh Nopember
2020

[Halaman ini sengaja dikosongkan]

LEMBAR PENGESAHAN TESIS

Tesis disusun untuk memenuhi salah satu syarat memperoleh gelar
Magister Komputer (M.Kom)
di
Institut Teknologi Sepuluh Nopember
Oleh:

M U R D I O N O
NRP: 05211650010027

Tanggal Ujian: 15 Januari 2020
Periode Wisuda: Maret 2020

Disetujui oleh:
Pembimbing:

1. Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom. .....
   NIP: 19730219 199802 1001

Penguji:

1. Dr. Apol Pribadi Subriadi, ST., MT. .....
   NIP: 19700225 200912 1 001

2. Nur Aini Rakhmawati, S.Kom. M.Sc.Eng., Ph.D. .....
   NIP: 19820120 200501 2 001

Kepala Departemen Sistem Informasi
Fakultas Teknologi Elektro Dan Informatika Cerdas

Dr. Mudjahidin, ST., MT.
NIP: 19701010 200312 1001

[Halaman ini sengaja dikosongkan]

Penyusunan Kebijakan Keamanan Informasi Dengan Penilaian Risiko Keamanan Aset Pada Kampus Institut Teknologi Sepuluh Nopember Berdasar Standar ISO 27001

Nama mahasiswa : Murdiono

NRP : 05211650010027

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

ABSTRAK

Informasi adalah aset bagi organisasi, hilang atau rusaknya informasi dapat berakibat matinya organisasi. Seiring dengan perkembangan zaman, semakin meningkat pula ancaman terhadap keamanan informasi. Hal ini dapat dibuktikan laporan yang diterbitkan oleh Symantec ISRT (*Internet Security Threat Report*) dimana setiap tahun jumlah ancaman yang terjadi terus meningkat. Oleh sebab itu pada organisasi diperlukan implementasi sistem manajemen keamanan informasi (SMKI) sebagai salah satu strategi dalam menjalan organisasi. Di dalam implementasi SMKI organisasi komponen utama yang harus disediakan yaitu kebijakan keamanan informasi (KKI) yang digunakan sebagai landasan berpijak dalam pengelolaan informasi organisasi.

Institut Teknologi Sepuluh Nopember (ITS) Surabaya, merupakan salah satu universitas yang telah mengandalkan teknologi informasi sebagai strategi organisasi. Dalam pengembangan teknologi informasi kampus, ITS telah mengimplementasikan *Single Sign On* (SSO) pada sistem integrasi sistem informasi yang ada kampus. Namun sayangnya implementasi SSO tersebut belum diimbangi dengan SMKI yang sempurna. Hal ini dikarenakan pada kampus ITS belum mempunyai dokumen KKI yang dapat digunakan sebagai landasan pengelolaan informasi dan untuk pengamanan informasi masih mengandalkan tool keamanan yang ada.

Tujuan dari penelitian ini adalah untuk membangun KKI pada kampus ITS dengan melakukan penilaian aset informasi, manajemen risiko dan mitigasinya berdasar standar ISO 27001. *Output* dari penelitian ini adalah draf KKI yang diharapkan dapat disetujui oleh manajemen ITS dan dapat dijadikan dasar hukum pengelolaan sistem informasi di kampus ITS.

Kata Kunci : *Kebijakan Keamanan, Keamanan Informasi, ISO 27001, Strategi, SMKI*

[Halaman ini sengaja dikosongkan]

Information Security Policy Development using Asset Risk Assessment at Sepuluh Nopember Institute of Technology Based on ISO 27001 Standards

Name : Murdiono

NRP : 05211650010027

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

ABSTRACT

Information is an asset for the organization, loss or destruction of information can result in the death of the organization. Along with the times, there are also increasing challenges to information security. This can be proven based on a report released by Symantec ISRT (Internet Security Threat Report) where each year the number continues to increase. Therefore in the organization required the implementation of an information security management system (ISMS) as one of the strategies in running the organization. In the implementation of the ISMS, the main component organizations must provide an information security policy (ISP) which is used as a basis for managing the organization's information.

Sepuluh Nopember Institute of Technology (ITS) Surabaya, is one of the universities that has relied on information technology as an organizational strategy. In developing campus information technology, ITS has implemented Single Sign On (SSO) on the existing campus information system integration system. The SSO implementation has not been matched by a perfect ISMS. This relates to the ITS campus which does not yet have ISP documents that can be used as an information base and for information security that still relies on existing security tools.

The purpose of this study is to develop the ISP on the ITS by conducting an risk assessment of information assets, risk management and mitigation based on ISO 27001 standards. The output of this study is a draft of the ISP documents that is expected to be used by ITS management and can be used for legal information systems at the ITS.

Keyword : *Security Policy, Informatiom Security, ISO 27001, Strategy, ISMS*

[Halaman ini sengaja dikosongkan]

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Allah SWT, yang telah memberikan ridho, rahmat, dan hidayah-nya sehingga tesis yang berjudul "Penyusunan Kebijakan Keamanan Informasi Dengan Penilaian Risiko Keamanan Aset Pada Kampus Institut Teknologi Sepuluh Nopember Berdasar Standar ISO 27001" dapat disusun dengan baik. Tesis ini disusun sebagai salah satu syarat menyelesaikan pendidikan pada Program Magister Sistem Informasi, Jurusan Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember.

Dalam proses penyelesaian tesis ini, penulis mendapatkan banyak bantuan, baik bantuan moral maupun materiil dari berbagai pihak. Oleh karena itu, penulis mengucapkan banyak terimakasih kepada :

1. Orang tua penulis, Bpk. Kasim dan Ibu (alm.) Murtini, yang selalu memberikan doa dan dukungan selama menyelesaikan studi dan tesis ini.
2. Istri tercinta dan anak-anakku yang sholih dan sholihah, tanpa dukungan kalian mustahil tesis ini dapat terselesaikan.
3. Bapak Dr.Eng. Febriliyan Samopa, S.Kom., M.Kom, selaku dosen pembimbing dan Dosen Wali Akademik yang telah meluangkan waktu, tenaga dan pikiran, serta memberikan ilmu, dukungan, dan kesabaran selama membimbing penulis dawi awal hingga tesis ini selesai.
4. Bapak Dr. Apol Pribadi Subriadi, ST., MT., selaku Dosen Penguji I yang telah bersedia menguji dan memberikan masukan untuk penelitian ini.
5. Ibu Nur Aini Rakhmawati, S.Kom. M.Sc.Eng., Ph.D., selaku Dosen Penguji II yang telah bersedia menguji dan memberikan masukan untuk penelitian ini.
6. Bapak Royyana Muslim Ijtihadie, S.Kom., M.Kom., Ph.D., Ibu Anny Yuniarti, S.Kom., M.Comp.Sc., Bapak Rizky Januar Akbar, S.Kom., M.Eng. dan Bapak Cahya Purnama Dani, A.Md. selaku manajemen DPTSI ITS yang telah bersedia meluangkan waktu dan tenaga sebagai narasumber hingga terselesaikannya tesis ini.

7. Bapak Imam Baihaqi, S.T., M.Sc., Ph.D., Bapak Nugroho Priyo Negoro, ST., SE., MM., Bapak Berto Mulia Wibawa, S.Pi., MM. dan Ibu Dr.oec.HSG Syarifa Hanoum, S.T., MT., selaku jajaran menejemen Departemen Manajemen Bisnis ITS yang selalu mendorong dan menberikan banyak kemudahan didalam pelaksanaan pengerjaan tesis ini.
8. Bapak Sugeng Djoko, Ibu Herlin Prihartati dan rekan-rekan Departemen Manjemen Bisnis ITS atas bantuan doa dan dukungannya.
9. Rekan-rekan DKM Nur Mudrikah, terima kasih sumbang semangat dan doa yang diberikan.
10. Teman-teman S2 Sistem Informasi angkatan 2016, khususnya mas Nasrullah yang selalu memingatkan dan memberikan semangat untuk bisa segera menyelesaikan tesis ini.
11. Mbak Vian (Irvian Ayu Novani), sekali staf Akdemik S2 Dept. Sistem Informasi yang selalu saya repoti selama kuliah di S2 Sistem Informasi
12. Dan semua pihak yang telah membantu terselesaikannya tesis ini dan tidak bisa saya sebut satu per satu. Semoga amal ibadah seluruh pihak yang tekah membantu saya mendapatkan balasan kebaikan oleh Allah SWT. Aaamiin..

DAFTAR ISI

[Halaman ini sengaja dikosongkan]

DAFTAR GAMBAR

[Halaman ini sengaja dikosongkan]

DAFTAR TABEL

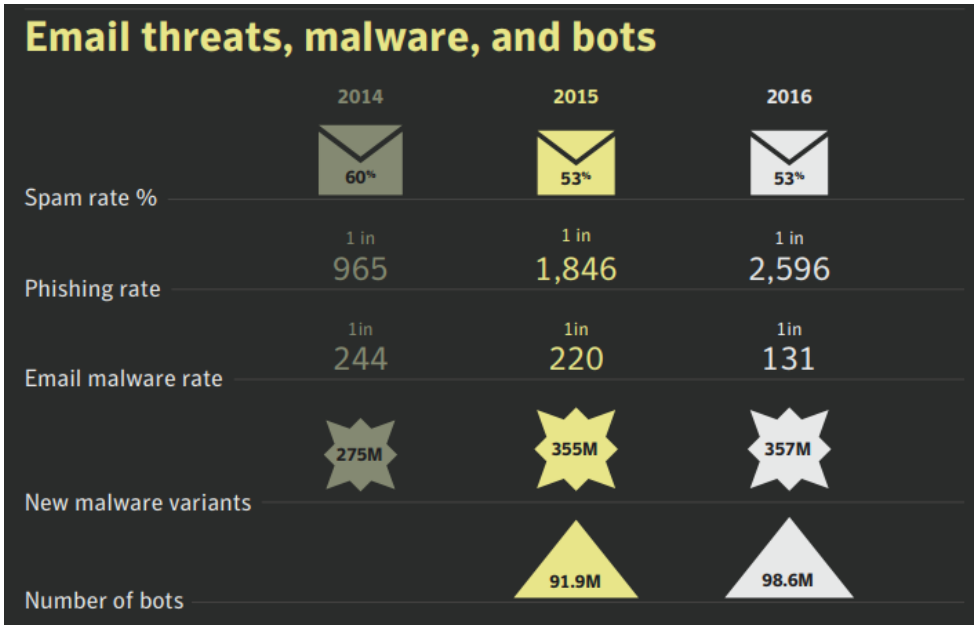
BAB 1
PENDAHULUAN

1.1 Latar Belakang

Di era komputerisasi saat ini, informasi merupakan suatu aset bagi suatu organisasi atau perusahaan. Informasi semakin diakui sebagai salah satu aset perusahaan yang paling berharga, walaupun pada kenyataannya informasi tidak dapat dihitung secara kuantitatif serta tidak dapat dimasukkan ke dalam neraca perusahaan (Moody and Walsh, 1999). Untuk itu organisasi wajib menjaga keutuhan, keakuratan dan ketersediaan informasi yang memadai guna menjaga keberlangsungan dan kesuksesan organisasi di masa depan.

Seiring dengan perkembangan teknologi informasi, masalah keamanan informasi juga semakin meningkat. Ancaman terhadap keamanan informasi memiliki aneka jenis dan bentuk bergantung dari tujuan diciptakannya ancaman tersebut. Dari tahun ke tahun, jumlah dan jenis ancaman terhadap keamanan informasi semakin meningkat. Berdasar laporan Symantec ISRT (*Internet Security Threat Report*) tahun 2017 terjadi peningkatan pada ancaman jenis *Phishing* dari angka 1.846 pada tahun 2016 menjadi 2.596 di tahun 2017. Begitu pula dengan ancaman jenis *Malware* terjadi peningkatan jumlah varian baru, yaitu dari angka 355juta pada tahun 2016 menjadi 357 juta varian di tahun 2017. Selain itu terjadi peningkatan jumlah ancaman berupa bots dari angka 91.9 juta pada tahun 2016 naik menjadi 98.6 juta di tahun 2017. Untuk lebih jelasnya terkait peningkatan jumlah ancaman keamanan dapat dilihat pada gambar 1.1. (*ISTR 2017*, 2017).

Untuk meminimalkan dampak kerusakan ataupun kehilangan informasi dari banyaknya ancaman yang muncul maka diperlukan suatu sistem yang mampu mengatur semua proses pengamanan informasi pada organisasi yang biasa disebut dengan Sistem Manajemen Keamanan Informasi (SMKI).



Gambar 1.1 Jumlah Ancaman Keamanan Informasi berdasar Symantec ISTR 2017 (Internet Security Threat Report)

Dalam sebuah organisasi, mengelola keamanan informasi sama pentingnya dengan mengelola bisnis inti. Itulah sebabnya mengapa organisasi bisnis sekarang lebih mengkhawatirkan keamanan informasi mereka. Oleh karena peran SMKI sangatlah penting yaitu menciptakan dan memelihara lingkungan informasi yang aman pada organisasi. Dalam membangun SMKI tidaklah mudah, harus ada analisis dan desain yang tepat dan melibatkan semua komponen organisasi. Hal ini karena SMKI merupakan salah satu keputusan perusahaan yang paling strategis dan landasan keamanan informasi dalam suatu organisasi (Dey, 2007). Pernyataan yang serupa juga disampaikan oleh Mirela (Mirela and Maria, 2008) yang menyebutkan bahwa SMKI memainkan peran penting untuk melindungi organisasi dan kemampuan untuk menjalankan misi bisnis organisasi, bukan hanya melindungi aset informasi saja. Adanya SMKI merupakan keputusan strategis dari suatu organisasi, pengembangan dan implementasi sistem yang dipengaruhi oleh kebutuhan dan tujuan strategis dari entitas organisasi.

Menutur pandangan The ENISA (*European Network and Information Security Agency*), dalam membangun SMKI pada organisasi terdapat kerangka kerja yang terdiri atas 6 tahapan yang harus dikerjakan agar SMKI dapat terwujud dengan benar. Adapun tahapan tersebut yaitu:

(1) Mendefinisikan Kebijakan Keamanan Informasi;

(2) Mendefinisikan ruang lingkup SMKI;

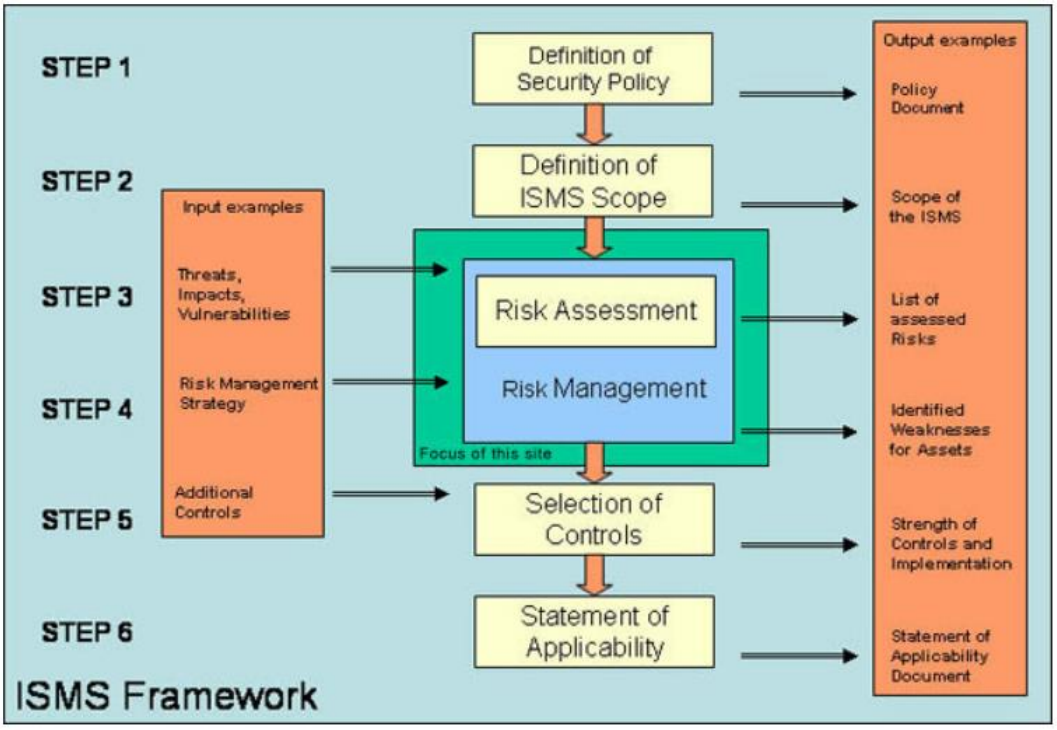
(3) Penilaian Risiko;

(4) Manajemen Risiko;

(5) Seleksi Kontrol dan

(6) Penyataan Penerapan SMKI (Mirela and Maria, 2008).

Model Kerangka Kerja SMKI yang dijelaskan oleh The UNISA tersebut dapat dilihat pada gambar 1.2 dibawah ini:



Gambar 1.2 Kerangka Kerja SMKI (Mirela and Maria, 2008).

Dari kerangka kerja pengembangan SMKI tersebut sangatlah jelas bahwa langkah pertama yang harus dilakukan dalam pengembangan SMKI pada organisasi yaitu membangun dan/atau mendefinisikan kebijakan keamanan. Mirela pun menjelaskan bahwa pendefinisian kebijakan keamanan dan ruang lingkup SMKI merupakan bagian dari manajemen dan strategi organisasi.

Dalam pengembangan dan pelaksanaan SMKI, kebijakan keamanan informasi berperan sebagai landasan dan pijakan hukum satu level dibawah regulasi

yang telah ditetapkan oleh pemerintah ataupun standar industri (Laudon and Traver, 2016). Dokumen kebijakan keamanan informasi menjadi dokumen paling penting dalam lingkungan organisasi ketika SMKI dijalankan (Peltier, 2002). Dokumen kebijakan keamanan informasi juga akan memberikan fondasi di mana setiap inisiatif keamanan informasi di organisasi harus dibangun (Etsebeth, 2006).

Gambar 1.3 Multi-layer pengamanan data/informasi (Laudon and Traver, 2016)

Menurut Mcllwraith, kebijakan keamanan informasi memiliki 3 (tiga) peran utama, yaitu:

(1) Penghapusan ambiguitas – kebijakan keamanan dapat digunakan sebagai pembatas keputusan manajemen organisasi yang dianggap membingungkan;

(2) Penjelas tujuan - kebijakan keamanan memberikan penjelas atas apa yang harus dilakukan dan apa yang harus dihilangkan;

(3) Penyeimbang antara keterbukaan dan perlindungan – kebijakan keamanan memberikan peran membantu menentukan kebutuhan bisnis perusahaan dengan memberikan definisi kejelasan keamanan di dalamnya (McIlwraith, 1993).

Bahkan menurut Solms, salah satu dari 10 (sepuluh) dosa besar dalam implementasi keamanan informasi yaitu : Tidak menyadari bahwa kebijakan keamanan informasi organisasi sangat penting (Von Solms and Von Solms, 2004).

Dengan begitu pentingnya kedudukan kebijakan keamanan informasi yang tertulis dalam dokumen kebijakan keamanan yang terlegalisir maka dapat diambil simpulan bahwa dokumen kebijakan keamanan informasi harus ada pada setiap organisasi yang menjadi informasi sebagai salah satu aset utamanya. Menurut Pelter, terdapat 5 (lima) konsekuensi utama yang dapat terjadi pada suatu organisasi jika tidak memiliki kebijakan ini: (i) Hilangnya keunggulan kompetitif; (ii) Kehilangan kepercayaan pelanggan dan pemegang saham; (iii) Meningkatnya campur tangan pemerintah; (iv) Ketidakpatuhan terhadap persyaratan legislatif; dan (v) Risiko pertanggung-jawaban hukum meningkat (Peltier, 2002).

Kampus Institut Teknologi Sepuluh Nopember (ITS) Surabaya merupakan salah satu kampus ternama di Indonesia yang telah menjadikan teknologi sistem informasi (TSI) sebagai strategi mencapai tujuan organisasi. Hal ini disebutkan secara jelas pada Misi ITS yang berbunyi memberikan kontribusi nyata dalam pengembangan ilmu pengetahuan, teknologi dan seni untuk kesejahteraan masyarakat melalui kegiatan-kegiatan pendidikan, penelitian, pengabdian kepada masyarakat dan pengelolaan sistem berbasis Teknologi Informasi dan Komunikasi (TIK). Misi tersebut selaras dengan tujuan strategis kampus ITS yaitu menuju *university resource planning* dan *world class university* (*Renstra ITS 2014 - 2018*, 2014).

Dalam salah satu langkah inisiatif strategi ITS dibidang sumber daya TSI adalah membentuk satu Portal ITS yang dijadikan sebagai pintu gerbang pemberian e-layanan (*e-service*) kepada seluruh pemangku kepentingan di ITS. Hal tersebut saat ini telah terwujud dengan diimplementasikannya Aplikasi ITS Integra (MyITS) yaitu aplikasi yang berfungsi sebagai gerbang utama untuk membuka dan menjalankan sistem informasi lainnya yang ada di ITS, seperti SIM Akademik, SIM Keuangan, SIM kepegawaian dan sistem-sistem khusus lainnya dengan menggunakan sistem *single sign-on* (SSO) yaitu penerapan satu *user* dan satu *password* untuk mendapatkan semua layanan Sistem Informasi di ITS. Tujuan implementasi sistem *single sign-on* pada Sistem Informasi Integra ini adalah untuk memudahkan pengguna di dalam mengakses semua sistem informasi yang ada pada kampus ITS, yaitu dengan sekali login maka pengguna dapat mengakses semua Sistem Informasi yang ada di ITS sesuai dengan peran dan tanggung jawab masing-

masing pengguna tanpa harus login dan mengingat *user – password* untuk tiap-tiap sistem informasi.

Dengan mengimplementasikan sistem SSO pada aplikasi Integra ITS, maka peran SMKI haruslah berjalan. Tidak hanya pada level pengamanan aplikasi saja namun lebih jauh pada kebijakannya keamanan yang nyata. Menurut Solms (Von Solms, 1997), untuk mewujudkan implementasi Sistem SSO yang aman (*Secure SSO*) maka harus memenuhi 3 (tiga) persyaratan yaitu:

(i) Desain keamanan yang dirancang secara cermat;
(ii) Penegakan kebijakan keamanan (*security policy*) yang konsisten; dan
(iii) Kesamaan pandangan manajemen terhadap keamanan dan audit;

Namun pada kenyataannya kampus ITS sampai saat ini masih belum dapat menjalankan SMKI dengan sempurna. Hal ini dikarenakan sampai dengan saat ini kampus ITS masih belum mempunyai kebijakan keamanan yang tertulis dan terdokumentasi. Untuk melaksanakan pengamanan informasi yang ada di ITS saat ini, masih mengandalkan *tools* keamanan yang dimiliki dan juga prosedur keamanan yang tidak memiliki dasar acuan ketetapan hukum yang disahkan oleh manajemen. Untuk itulah diperlukan satu dokumen legal kebijakan keamanan yang disahkan oleh manajemen ITS sebagai dasar landasan pelaksanaan SMKI di kampus ITS.

Berdasar pengamatan dan wawancara non formal yang dilakukan oleh peneliti, banyak organisasi yang telah menggunakan teknologi informasi sebagai salah satu strategi dalam menjalankan proses bisnis mereka, namun mereka juga belum mempunyai kebijakan keamanan informasi sebagai landasan dalam pelaksanaan pengamanan informasi organisasi yang mereka kelola. Kondisi yang ada selama ini pada organisasi hanya mengandalkan teknik dan *tool* di dalam mengamankan aset informasi yang ada. Hal ini disebabkan kurangnya pemahaman manajemen tentang bagaimana mengimplementasikan kerangka SMKI yang ada, khususnya tentang peran kebijakan keamanan informasi pada organisasi.

Penelitian-penelitian yang telah ada belum mampu memberikan gambaran yang mendetail tentang langkah-langkah pengembangan kebijakan keamanan informasi yang sesuai dengan kondisi organisasi. Kerangka kerja pengembangan kebijakan keamanan informasi tersebut masih terlalu global dan tidak disertai

petunjuk teknis yang jelas. Selain itu masalah keterbatasan SDM dan anggaran juga masih menjadi masalah organisasi dalam pelaksanaan SMKI.

Untuk itu peneliti mencoba memberikan gambaran kerangka kerja pengembangan kebijakan keamanan informasi yang lebih konkrit berdasar standar dokumen ISO 27001:2013, sehingga dapat digunakan sebagai acuan oleh organisasi non-Enterprise untuk membangun kebijakan keamanan informasi mereka.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, maka uraian masalah yang ingin dijawab melalui penelitian ini yaitu:

a. Bagaimana menilai kondisi sistem manajemen keamanan informasi pada kampus ITS saat ini?
b. Bagaimana menyusun draf kebijakan keamanan informasi yang sesuai dengan kondisi SMKI dan kultur yang ada di kampus ITS?

1.3 Tujuan Penelitian

Berdasarkan perumusan masalah diatas, maka tujuan dari penelitian ini yaitu;

1. Melakukan penilaian risiko keamanan informasi yang ada pada Kampus ITS sesuai dengan kerangka kerja pengembangan keamanan informasi dan standar ISO 27001:2013.
2. Membantu pihak manajemen ITS dengan memberikan usulan draf kebijakan keamanan informasi yang sesuai dengan kondisi kampus ITS saat ini yang dapat dijadikan sebagai landasan pelaksanaan SMKI pada kampus ITS.

1.4 Batasan Penelitian

Di dalam pelaksanaan penelitian ini memiliki beberapa batasan. Adapun batasan tersebut adalah:

1. Objek dari penelitian ini adalah Direktorat Pengembangan Teknologi dan Sistem Informasi [DPTSI] ITS, selaku lembaga yang bertanggung jawab membuat dan mengelola seluruh sistem informasi dan teknologi informasi yang ada di ITS.

2. Standar dokumen yang dijadikan acuan penilaian SMKI dan penyusunan kebijakan keamanan informasi pada penelitian ini yaitu standar dokumen ISO 27001:2013 serta Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik yang dibuat oleh Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika Edisi: 2.0, September 2011.
3. Dasar Perundangan dan Peraturan pemerintah yang digunakan sebagai dasar pada pembuatan kebijakan keamanan pada penelitian ini, antara lain:
    - Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
    - Peraturan Pemerintah Republik Indonesia Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik.
    - Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik.
    - Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008.
    - Permen Komunikasi Dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.
    - Permen Komunikasi Dan Informatika Nomor: 41/Per/Men.Kominfo/11/2007 Tentang Panduan Umum Tata Kelola Teknologi Informasi Dan Komunikasi Nasional.
4. Luaran dari penelitian ini adalah draf dokumen kebijakan keamanan informasi yang ada akan diajukan ke manajemen ITS. Adapun dokumen tersebut yaitu:
    - Kebijakan Keamanan Informasi Umum

1.5 Kontribusi Penelitian

- **Kontribusi Keilmuan**

  Melakukan pembuktian penghitungan risiko keamanan informasi dengan berdasar pada standar ISO 27001 sesuai dengan literatur yang ada dan penelitian pendahulu yang telah dilakukan yang selanjutnya hasil dari penilaian tersebut dijadikan sebagai dasar penyusunan kebijakan keamanan organisasi.

- **Kontribusi Praktis**

  Hasil penelitian ini berupa draf kebijakan keamanan informasi yang sesuai dengan kondisi risiko keamanan yang ada pada kampus ITS, sehingga diharapkan dapat draf kebijakan tersebut dapat disahkan oleh manajemen ITS dan dijadikan sebagai landasan pelaksanaan SMKI pada kampus ITS

1.6 Sistematika Penulisan

Sistematika penulisan dokumen pada laporan penelitian ini dibagi menjadi 5 (lima) bab yakni sebagai berikut:

a. Bab 1 Pendahuluan

Bab ini terdiri dari latar belakang penelitian, perumusan masalah, tujuan penelitian, kontribusi penelitian, keterbaruan penelitian, batasan penelitian dan sistematika penulisan.

b. Bab 2 Kajian Pustaka

Bab ini berisi kajian yang meliputi teori-teori dan penelitian yang sudah ada terkait dengan topik penelitian.

c. Bab 3 Metodologi Penelitian

Bab ini membahas mengenai rancangan penelitian, lokasi dan tempat penelitian, dan juga tahapan-tahapan sistematis yang digunakan selama melakukan penelitian.

d. Bab 4 Hasil dan Pembahasan

Bab ini menjelaskan hasil dari penelitian serta pembahasan sesuai dengan penulisan kualitatif.

e. Bab 5 Kesimpulan dan Saran

Bab ini membahas mengenai kesimpulan dari penelitian yang telah dilakukan dan saran untuk pengembangan penelitian selanjutnya.

[Halaman ini sengaja dikosongkan]

BAB 2
KAJIAN PUSTAKA

Pada bab ini akan dibahas mengenai kajian pustaka dan dasar teori yang mendukung dalam pengerjaan penelitian.

2.1 Informasi Sebagai Aset

Informasi merupakan aset yang berharga bagi sebuah organisasi yang memiliki nilai dan menjadi salah satu ujung tombak kesuksesan organisasi, untuk itu sebagaimana aset-aset yang lain maka informasi pun harus dilindungi dan dijaga, sebab hilang atau bocornya informasi berharga pada organisasi akan mempengaruhi keberlangsungan organisasi tersebut.

Secara umum informasi dapat diartikan pesan (ucapan atau ekspresi) atau kumpulan pesan yang terdiri dari order sekuens dari simbol, atau makna yang dapat ditafsirkan dari pesan atau kumpulan pesan. Informasi dapat direkam atau ditransmisikan. Dalam bidang teknologi informasi dan komunikasi, Informasi diartikan kumpulan fakta yang dikelola sedemikian rupa sehingga memiliki nilai tambahan di luar nilai fakta itu sendiri (Stair and Reynolds, 2010). Informasi dapat disimpan dalam berbagai bentuk, termasuk: formulir digital (misalnya file data yang disimpan di media elektronik atau optik), bentuk materi (misalnya di atas kertas), serta informasi yang tidak ter wakilkan seperti pengetahuan karyawan. Informasi juga dapat dikirimkan dengan berbagai cara termasuk: kurir, komunikasi elektronik atau lisan.

Dari sekumpulan informasi yang dikelola oleh organisasi dapat menghasilkan pola pengetahuan berharga yang dapat digunakan untuk pengambilan keputusan organisasi. Informasi yang berharga tersebut dapat membantu organisasi melakukan tugas secara lebih efisien dan efektif.

2.2 Keamanan Informasi

Secara umum, keamanan berarti melindungi dari segala hal yang mengancam dan berbahaya. Menurut *The Committee on National Security Systems* (CNSS),

keamanan informasi adalah melindungi informasi dan elemen kritisnya, termasuk sistem dan perangkat keras yang digunakan, penyimpanan dan proses transmisi/pengiriman informasi tersebut (Whitman and Mattord, 2012).

Sedangkan menurut Andreas, keamanan informasi didefinisikan sebagai "melindungi informasi dan sistem informasi dari akses yang tidak sah, penggunaan, pengungkapan, gangguan, modifikasi, atau perusakan" (Andress and Leary, 2016). Dalam arti umum, keamanan berarti melindungi aset berharga organisasi. Hal ini dapat berarti melindungi informasi tersebut dari serangan melalui jaringan, bencana alam, kondisi lingkungan yang merugikan, gangguan listrik, pencurian atau vandalisme, atau keadaan yang tidak diinginkan lainnya.

Keamanan informasi dapat dicapai melalui penerapan perangkat kontrol yang berlaku yang dipilih berdasar proses manajemen risiko dan dikelola dengan menggunakan sistem manajemen keamanan informasi, termasuk di dalamnya yaitu penerapan kebijakan keamanan informasi, proses dan prosedur, penetapan struktur organisasi yang tepat serta pemilihan perangkat keras dan perangkat lunak yang tepat guna melindungi aset informasi yang dimiliki.

Kesuksesan dalam keamanan informasi tidak terlepas dari komponen keamanan yang mendukungnya. Menurut Whitman dan Mattord, terdapat beberapa komponen pendukung yang harus dilengkapi dalam meng-implementasikan keamanan informasi, yaitu:

- *Physical security*: keamanan yang memfokuskan strategi untuk mengamankan pekerja atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
- *Personal security*: keamanan yang *overlap* dengan *physical security* dalam melindungi orang-orang dalam suatu organisasi.
- *Operational security*: keamanan yang memfokuskan strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan.
- *Communications security*: keamanan yang bertujuan untuk mengamankan media komunikasi, teknologi komunikasi beserta isinya, dan kemampuan untuk memanfaatkan alat ini untuk mencapai tujuan sebuah organisasi.

- *Network security*: keamanan yang memfokuskan pada pengamanan peralatan jaringan dan organisasi, jaringan dan isinya, beserta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi tersebut.

Di dalam standar industri keamanan terdapat konsep klasik yang menjadi tujuan utama (*goal*) dari keamanan informasi yang biasa disebut dengan istilah C.I.A Triad, yang merupakan kepanjangan dari *confidentiality*, *integrity* dan *availability* yang ditunjukkan pada gambar 2.1. Artinya setiap informasi dikatakan aman bila ketiga aspek tersebut terpenuhi, yaitu kerahasiaan (*confidentiality),* Keutuhan *(integrity)* dan ketersediaan *(availability)* dengan penjabaran sebagai berikut:

- *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.
- *Integrity* (keutuhan) 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.
- *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).

Gambar 2.1 Diagram CIA Triad

Dari konsep CIA Triad ini, pada tahun 2002 Donn Parker mengusulkan tambahan tiga aspek komponen untuk keamanan informasi: *Possesion* (kepemilikan), *Utility* (utilitas), dan (*Authenticity*) keaslian. Kelompok baru yang dihasilkan dari enam komponen yang merupakan aspek keamanan informasi disebut sebagai Parkerian hexad (Raggad, 2010) . Adapun penjabaran dari ketiga komponen tambahan dalam Parkerian Hexad adalah sebagai berikut:

- *Possesion*, adalah terkait aspek kepemilikan dan kontrol terhadap informasi. Contoh, seorang pencuri telah mencuri amplop tersegel yang berisi kartu debit bank dan data pribadi kepemilikannya, walaupun si pencuri tidak membuka amplop tersebut, namun pemilik kartu pasti khawatir karena pencuri dapat kapan saja membuka dan mengakses informasi perbankan tersebut. Kondisi seperti inilah yang disebut sebagai *Loss Possesion* (kehilangan kontrol atas informasi yang dikuasai).
- *Utility*, menekankan kegunaan informasi dalam kepemilikan. Jika informasi ini tersedia dalam bentuk terenkripsi tetapi kita tidak memiliki cara untuk mendekripsi-nya, maka informasi tersebut tidak berguna bagi kita. Contoh lain adalah menerima pesan atau peringatan yang ditulis dalam bahasa asing yang tidak dapat kita pahami adalah bentuk pelanggaran utilitas.
- *Authenticity*, bertujuan untuk memastikan bahwa asal transmisi informasi adalah benar dan begitu juga dengan kepemilikan dokumen yang dikirimkan adalah valid.

Selain aspek keamanan informasi diatas, di dalam bukunya Dr. Michael E.Whitman dan Herbert J. Mattord menuliskan 6 (enam) aspek keamanan yang harus diperhatikan yaitu adalah: (Whitman and Mattord, 2012)

- *Privacy*

  Informasi yang dikumpulkan, digunakan, dan disimpan oleh organisasi adalah dipergunakan hanya untuk tujuan tertentu, khusus bagi pemilik data saat informasi ini dikumpulkan. *Privacy* menjamin keamanan data bagi pemilik.
- *Identification*

  Sistem informasi memiliki karakteristik identifikasi jika bisa mengenali individu pengguna. Identifikasi adalah langkah pertama dalam memperoleh hak

akses ke informasi yang diamankan. Identifikasi secara umum dilakukan dalam penggunaan *username* atau *user* ID.

- *Authentication*

  Autentikasi terjadi pada saat sistem dapat membuktikan bahwa pengguna memang benar-benar orang yang memiliki identitas yang mereka klaim.

- *Authorization*

  Setelah identitas pengguna diautentikasi, sebuah proses yang disebut autorisasi memberikan jaminan bahwa pengguna (manusia ataupun komputer) telah mendapatkan autorisasi secara spesifik dan jelas untuk mengakses, mengubah, atau menghapus isi dari aset informasi.

- *Accountability*

  Karakteristik ini dipenuhi jika sebuah sistem dapat menyajikan data semua aktivitas terhadap aset informasi yang telah dilakukan, dan siapa yang melakukan aktivitas itu.

2.3 Manajemen Keamanan Informasi

Dalam rangka untuk mengamankan aset informasi pada organisasi maka semestinya sebuah organisasi haruslah menerapkan manajemen keamanan informasi.

Manajemen keamanan informasi adalah suatu proses yang mampu (1) secara akurat mengidentifikasi lingkungan komputasi organisasi, mendefinisikan tingkat kekritisannya, dan memprioritaskan kontribusinya untuk nilai bisnis organisasi; (2) secara akurat mengidentifikasi semua risiko keamanan, menilai semua kelemahan dan ancaman, dan kemudian memitigasi risiko tersebut dengan merancang program keamanan berbasis risiko yang komprehensif; serta (3) menyediakan peningkatan berkelanjutan dari posisi risiko organisasi dengan secara otomatis merevisi program keamanan yang digerakkan oleh risiko seiring dengan perubahan tingkat keamanan informasi dengan perubahan dalam lingkungan komputasi organisasi. (Raggad, 2010).

Sedang definisi manajemen keamanan infromasi menurut ISO/IEC 27000 yaitu proses manajemen yang meliputi pembuatan, pengawasan dan pengambilan keputusan yang diperlukan untuk mencapai tujuan bisnis melalui perlindungan aset

informasi organisasi. Manajemen keamanan informasi diungkapkan melalui perumusan dan penggunaan kebijakan keamanan informasi, prosedur dan pedoman, yang kemudian diterapkan di seluruh organisasi oleh semua individu yang terkait dengan organisasi. ("ISO/IEC 27000:2016(E)," 2016).

Di dalam bukunya yang berjudul "*Management of Information Security",* Whitman dan Mattord menyebutkan terdapat 6 (enam) karakter yang harus dimiliki dalam melakukan manajemen keamanan informasi (Whitman and Mattord, 2014). Keenam karakter tersebut dikenal dengan istilah " *The Six P's*", yaitu (*planning, policy, programs, protection, people,* dan *project management*) yang dijabarkan sebagai berikut:

- ***Planning***

Planning dalam manajemen keamanan informasi meliputi proses perancangan, pembuatan, dan implementasi strategi untuk mencapai tujuan. Ada tiga tahapannya yaitu:

1) *strategic planning* yang dilakukan oleh tingkatan tertinggi dalam organisasi untuk periode yang lama, biasanya lima tahunan atau lebih,
2) *tactical planning* memfokuskan diri pada pembuatan perencanaan dan mengintegrasi sumber daya organisasi pada tingkat yang lebih rendah dalam periode yang lebih singkat, misalnya satu atau dua tahunan,
3) *operational planning* memfokuskan diri pada kinerja harian organisasi. Sebagai tambahannya, planning dalam manajemen keamanan informasi adalah aktivitas yang dibutuhkan untuk mendukung perancangan, pembuatan, dan implementasi strategi keamanan informasi supaya diterapkan dalam lingkungan teknologi informasi.

- ***Policy***

Dalam keamanan informasi, ada tiga kategori umum dari kebijakan keamanan informasi yaitu:

1) *Enterprise Information Security Policy (EISP)* menentukan kebijakan departemen keamanan informasi dan menciptakan kondisi keamanan informasi di setiap bagian organisasi.
2) *Issue Spesific Security Policy (ISSP)* adalah sebuah peraturan yang menjelaskan perilaku yang dapat diterima dan tidak dapat diterima dari segi

keamanan informasi pada setiap teknologi yang digunakan, misalnya email atau penggunaan internet.

3) *System Spesific Policy (SSP)* pengendali konfigurasi penggunaan perangkat atau teknologi secara teknis atau manajerial.

- ***Programs***

Adalah operasi-operasi dalam keamanan informasi yang secara khusus diatur dalam beberapa bagian. Salah satu contohnya adalah program *security education training and awareness*. Program ini bertujuan untuk memberikan pengetahuan kepada pekerja mengenai keamanan informasi dan meningkatkan pemahaman keamanan informasi pekerja sehingga dicapai peningkatan keamanan informasi organisasi.

- ***Protection***

Fungsi proteksi dilaksanakan melalui serangkaian aktivitas manajemen risiko, meliputi perkiraan risiko (*risk assessment*) dan pengendali, termasuk mekanisme proteksi, teknologi proteksi dan perangkat proteksi baik perangkat keras maupun perangkat keras. Setiap mekanisme merupakan aplikasi dari aspek-aspek dalam rencana keamanan informasi.

- ***People***

Manusia adalah penghubung utama dalam program keamanan informasi. Penting sekali mengenali aturan krusial yang dilakukan oleh pekerja dalam program keamanan informasi. Aspek ini meliputi personil keamanan dan keamanan personil dalam organisasi.

- ***Project Management***

Komponen terakhir adalah penerapan kedisiplinan manajemen dalam setiap elemen keamanan informasi. Hal ini melibatkan identifikasi dan pengendalian sumber daya yang dikerahkan untuk keamanan informasi, misalnya pengukuran pencapaian keamanan informasi dan peningkatannya dalam mencapai tujuan keamanan informasi.

2.4 *Critical Success Factor* untuk Manajemen Keamanan Informasi

Di dalam implementasi manajemen keamanan informasi terdapat 12 (dua belas) *Critical Success Factor* yang digunakan untuk mengukur efektivitas dari

keamanan informasi yang diterapkan (Torres et al., 2006). Adapun penjabaran dari ke-12 *Critical Success Factor* tersebut adalah:

a. Arsitektur Keamanan IS

   Didefinisikan sebagai cara bagaimana struktur perangkat keras dan perangkat lunak yang ada pada organisasi diperkenalkan, diatur, dilindungi dan digunakan. Keandalan keamanan informasi dimulai dari desain arsitektur keamanan yang tepat dan kuat.

b. Koneksi Bisnis

   Ditetapkan sebagai koneksi eksternal dan internal ke intranet (jaringan) organisasi atau data penting organisasi.

c. Strategi Keamanan Informasi

   Ditetapkan sebagai proses peningkatan manajemen keamanan informasi yang terencana dan terstruktur. Ini termasuk memiliki rencana aksi, ruang lingkup, sumber daya, tim implementasi, tanggung jawab, dan waktu penyelesaian yang realistis dari manajemen keamanan informasi untuk tujuan yang telah ditetapkan.

d. Evaluasi dinamis terhadap efektivitas keamanan informasi

   Didefinisikan sebagai evaluasi berkelanjutan dari efektivitas manajemen keamanan sistem informasi. Memahami dan mengelola mekanisme dinamis yang mengontrol perilaku keamanan informasi.

e. Penilaian risiko

   Didefinisikan sebagai identifikasi akurat, klasifikasi dan penentuan prioritas aset penting, kerentanan, ancaman, dampaknya, dan kemungkinan yang akan terjadi.

f. Integrasi keamanan informasi

   Didefinisikan sebagai hubungan antara keamanan informasi dan kegiatan inti dan proses organisasi dengan tujuan menyelaraskan keamanan informasi dengan tujuan bisnis.

g. Pencapaian Proyek

   Didefinisikan sebagai tingkat di mana memulai strategi keamanan informasi, operasional dan teknis terpenuhi dan ditegakkan.

h. Penegakan Hukum dan Kepatuhan

   Didefinisikan sebagai tingkat penegakan dan kepatuhan terhadap kontrol keamanan informasi yang diimplementasikan.

i. Anggaran keamanan Informasi

   Didefinisikan sebagai persentase anggaran organisasi terhadap sumber daya TI yang didedikasikan untuk keamanan informasi.

j. Kesadaran Keamanan Informasi

   Didefinisikan sebagai penghargaan pada semua tingkatan dalam organisasi tentang kebutuhan dan manfaat keamanan informasi.

k. Komitmen Manajemen

   Didefinisikan sebagai tingkat pemahaman dan dukungan dari manajemen puncak tentang dampak keamanan informasi pada masa depan bisnis dan pemangku kepentingan.

l. Kompetensi Administrator dan pengguna

   Didefinisikan sebagai pengetahuan dan keterampilan IT yang dapat digunakan untuk memanfaatkan dan mengamankan IS dengan benar.

2.5 Sistem Manajemen Keamanan Informasi

Sistem Manajemen Keamanan Informasi (SMKI) atau dalam bahasa inggris disebut juga *Information Security Management System* (ISMS) adalah sebuah sistem yang harus diimplementasikan dengan hati-hati untuk mengatasi ancaman keamanan yang ada dan yang akan datang. SMKI adalah hasil dari salah satu keputusan perusahaan yang paling strategis dan landasan keamanan informasi dalam suatu organisasi (Dey, 2007).

Sedangkan menurut Eloff, Suatu Sistem Manajemen Keamanan Informasi dapat didefinisikan sebagai sistem manajemen yang digunakan untuk membangun dan memelihara lingkungan informasi yang aman. SMKI harus membahas implementasi dan pemeliharaan proses dan prosedur untuk mengelola keamanan Teknologi Informasi. Tindakan ini termasuk identifikasi kebutuhan keamanan informasi, penerapan strategi untuk memenuhi kebutuhan ini, pengukuran hasil, dan meningkatkan baik strategi perlindungan dan manajemen keamanan informasi dari waktu ke waktu (Eloff and Eloff, 2003).

Dalam makalahnya, Mirela mengutip dokumen ISO/IEC 27001:2005 yang mendefinisikan SMKI adalah bagian dari sistem manajemen global, berdasar pendekatan tertentu dari risiko bisnis, termasuk didalamnya adalah proses menetapkan, menerapkan, menganalisis, memantau, dan meningkatkan keamanan informasi. Sistem ini mencakup struktur organisasi, politik, kegiatan perencanaan, praktik, proses dan sumber daya. Keamanan informasi harus menjadi bagian integral dari budaya operasi dan bisnis organisasi (Mirela and Maria, 2008).

Dalam dunia yang saling terhubung, informasi dan proses, sistem, dan jaringan terkait merupakan aset bisnis penting. Organisasi, sistem informasi dan jaringan akan menghadapi ancaman keamanan dari berbagai sumber, termasuk penipuan yang dibantu komputer, spionase, sabotase, vandalisme, kebakaran, dan banjir. Kerusakan sistem informasi dan jaringan yang disebabkan oleh kode berbahaya, peretasan komputer, dan penolakan serangan layanan telah menjadi lebih umum, lebih ambisius, dan semakin canggih.

Dalam industri apa pun, SMKI adalah *enabler* yang mendukung e-bisnis dan sangat penting untuk kegiatan manajemen risiko. Interkoneksi jaringan publik serta proses berbagi aset informasi meningkatkan kesulitan mengendalikan akses dan penanganan informasi. Selain itu, distribusi perangkat penyimpanan bergerak (*mobile*) yang mengandung aset informasi dapat melemahkan efektivitas kontrol. Ketika organisasi mengadopsi standar SMKI, kemampuan untuk menerapkan prinsip keamanan informasi yang konsisten dan dapat dikenali dapat ditunjukkan kepada mitra bisnis dan pihak yang berkepentingan lainnya.

Keberhasilan adopsi SMKI penting untuk melindungi aset informasi yang memungkinkan organisasi untuk:

a) Mencapai jaminan yang lebih besar bahwa aset informasinya dilindungi secara memadai terhadap ancaman secara terus menerus;
b) Mempertahankan kerangka kerja yang terstruktur dan komprehensif untuk mengidentifikasi dan menilai risiko keamanan informasi, memilih dan menerapkan kontrol yang berlaku, dan mengukur serta meningkatkan efektivitasnya;
c) Secara terus menerus memperbaiki lingkungan pengendaliannya; dan
d) Secara efektif mencapai kepatuhan hukum dan peraturan.

2.6 Kerangka Kerja Sistem Manajemen Keamanan Informasi

Kerangka kerja pengembangan SMKI dapat didefinisikan sebagai satuan langkah / proses yang harus dikerjakan secara berurutan untuk mencapai tujuan utama yang mengamankan informasi.

The ENISA (*European Network and Information Security Agency*) adalah satu lembaga yang menawarkan konsep kerangka kerja SKMI (Mirela and Maria, 2008). Dalam kerangka kerja tersebut terdapat 6 tahapan yang harus dilaksanakan yaitu:

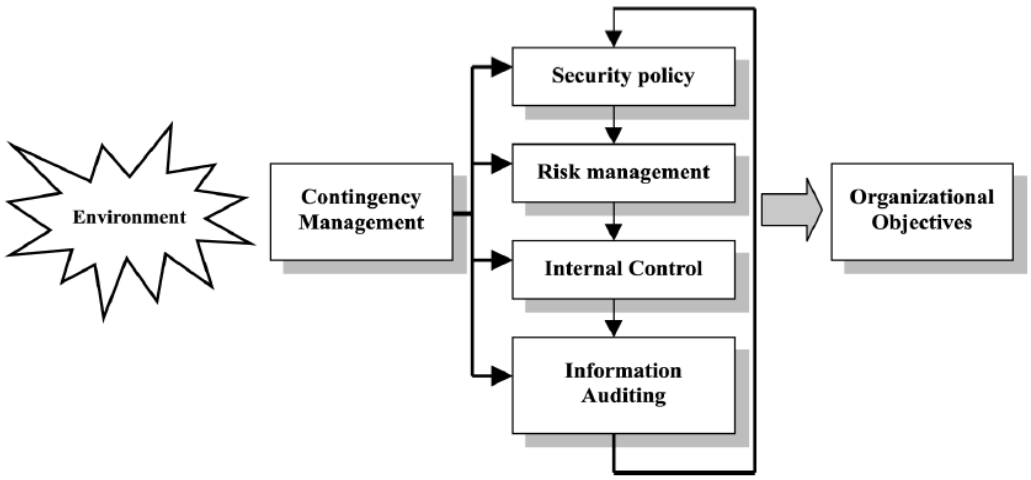
1. Mendefinisikan kebijakan keamanan
2. Menentukan ruang lingkup SMKI
3. Melakukan penilaian risiko
4. Manajemen risiko
5. Pemilihan kontrol yang tepat dan
6. Pernyataan keberlakuan.

Adapun desain diagram dari kerangka kerja SMKI yang ditawarkan oleh ENISA dapat dilihat pada gambar 1.2.

Sedangkan menurut Hong dalam penelitiannya menyebutkan bahwa untuk mencapai tujuan keamanan informasi, dibutuhkan implementasi dari integrasi teori dari keamanan informasi. Dalam konsepnya Hong menjelaskan ada 4 langkah kerangka SMKI yang ditujukan untuk mencapai tujuan organisasi. (Hong et al., 2003). Langkah-langkah tersebut adalah:

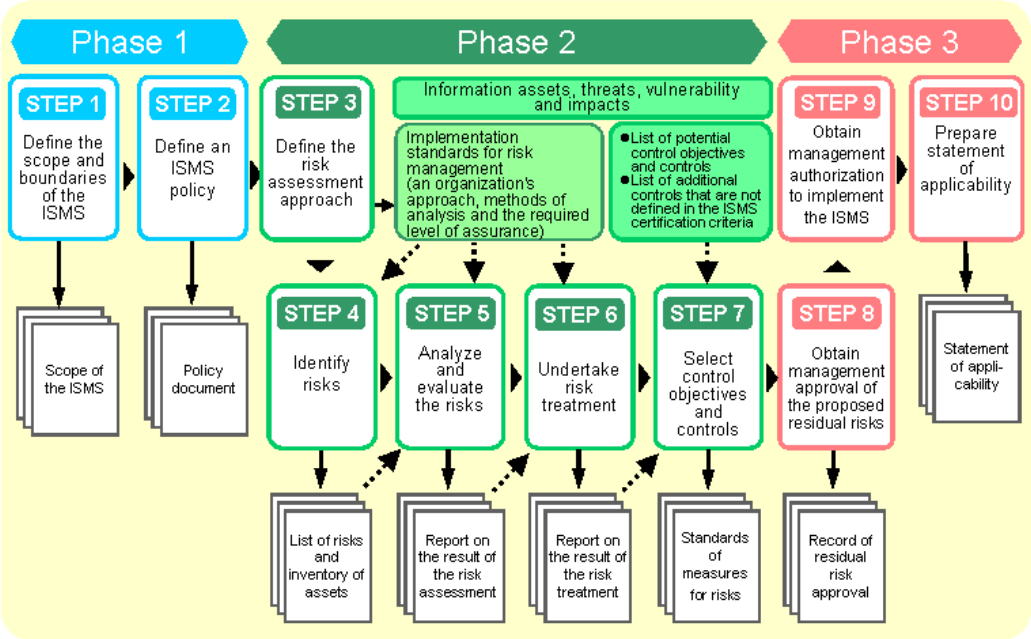
1. Kebijakan Keamanan
2. Manajemen Risiko
3. Kontrol Internal
4. Audit Informasi

Bagan diagram dari SMKI yang ditawarkan oleh Hong adalah sebagai berikut:



Gambar 2.2 Desain SMKI menurut Hong (Hong et al., 2003)

Sedangkan konsep kerangka kerja SMKI yang banyak diadopsi adalah kerangka kerja dari ISO / IEC 27001. Berdasar ISO 27001, terdapat 10 (sepuluh) langkah dalam membangun SMKI pada organisasi. Dalam menetapkan SMKI, dimulai dari menentukan ruang lingkup SMKI (langkah 1), dan kebijakan keamanan informasi didefinisikan (langkah 2). Atas dasar kebijakan keamanan ini, pendekatan sistematis untuk penilaian risiko didefinisikan (langkah 3), dan risiko terhadap aset informasi yang harus dilindungi diidentifikasi (langkah 4). Penilaian risiko kemudian dilakukan (langkah 5). Jika, sebagai hasil dari penilaian risiko, risiko yang tidak dapat diterima ditemukan, kemungkinan cara untuk menangani risiko harus diidentifikasi dan diperiksa (langkah 6). Berdasarkan perlakuan risiko, kontrol yang akan diterapkan dipilih (langkah 7). Setelah kontrol telah diterapkan pada semua risiko selanjutnya melalui manajemen risiko, risiko residual ini harus disetujui oleh Manajemen (langkah 8), dan juga pengenalan SMKI akan diizinkan oleh Manajemen (langkah 9). Dan langkah selanjutnya yaitu menentukan pemilihan kontrol dalam pernyataan penerapan (langkah 10).



Gambar 2.3 ISO 27001:2013 ISMS Framework (ISO 27001, 2013)

Dari ketiga model kerangka kerja SMKI tersebut, langkah yang menjadi dasar atau langkah yang pertama dilakukan adalah penyusunan dokumen kebijakan keamanan informasi. Hal ini menunjukkan betapa penting kebijakan keamanan informasi menjadi landasan dalam menjalankan manajemen keamanan infomasi secara keseluruhan dalam organisasi.

2.7 Kebijakan Keamanan Informasi

Menurut Meynard, Kebijakan keamanan informasi memaksa perusahaan untuk merencanakan kemungkinan bahwa sistem informasi mereka akan menjadi titik penyerangan, baik secara internal maupun eksternal. Dengan merencanakan kemungkinan serangan dan mengidentifikasi di mana serangan dapat terjadi, kebijakan keamanan memberlakukan perlindungan terhadap informasi organisasi.(Maynard and Ruighaver, 2002)

Menurut Whitman dalam bukunya yang berjudul "*Management of Information Security (4th Editions)*, menyatakan Kebijakan keamanan informasi adalah instruksi tertulis, yang disediakan oleh manajemen, untuk menginformasikan karyawan dan orang lain di tempat kerja tentang perilaku yang

tepat mengenai penggunaan informasi dan aset informasi. Kebijakan ini dirancang untuk menyediakan struktur di tempat kerja dan menjelaskan keinginan manajemen organisasi dalam mengendalikan perilaku karyawannya sehubungan dengan penggunaan sumber informasi dan informasi yang tepat dan aman. Kebijakan dirancang untuk menciptakan lingkungan kerja yang produktif dan efektif, bebas dari gangguan yang tidak perlu dan tindakan yang tidak pantas. (Whitman and Mattord, 2014)

Sedangkan menurut Ed Tittel, praktisi IT veteran yang pernah berkarir di IBM dan Schlumberger mengatakan bahwa kebijakan keamanan informasi / *security policy* dapat diartikan sebagai "sebuah aturan tertulis yang menerangkan bagaimana sebuah organisasi dapat melindungi aset bisnis dan teknologi informasinya". Dalam pandangannya, Ed mengatakan bahwa Kebijakan keamanan informasi ini adalah *living document*. Artinya, aturan tersebut akan selalu berkembang sesuai dengan perkembangan teknologi. Berdasarkan definisi Ed, dapat dikatakan bahwa mengembangkan security policy yang baik harus relevan dan sejalan dengan business plan yang telah disepakati sebelumnya. (Tittel, 2002)

Keberadaan dokumen "Kebijakan Keamanan" merupakan sebuah infrastruktur keamanan yang harus dimiliki oleh sebuah organisasi atau perusahaan yang ingin melindungi aset informasi terpentingnya. Dokumen ini secara prinsip berisi berbagai cara / kendali yang perlu dilakukan untuk mengontrol manajemen, mekanisme, prosedur, dan tata cara dalam mengamankan informasi, baik secara langsung maupun tidak langsung. Karena berada pada tataran kebijakan, maka dokumen ini biasanya berisi hal-hal yang bersifat prinsip dan strategis. Dengan adanya kebijakan ini, selain akan membantu organisasi dalam mengamankan aset pentingnya, juga menghindari adanya insiden atau tuntutan hukum akibat organisasi terkait lalai dalam melakukan pengelolaan internal terhadap aset informasi atau hal-hal terkait dengan tata kelola informasi yang berada dalam lingkungannya. Kebijakan yang dimaksud juga bersifat teknologi netral, artinya tidak tergantung atau spesifik terhadap penggunaan merek teknologi tertentu.

Elemen Kunci Kebijakan Keamanan EC-Council mendeskrisikan ada 7 (tujuh) elemen kunci yang harus diperhatikan dalam menyusun kebijakan

keamanan (EC-Council, 2010). 7 (tujuh) elemen kunci kebijakan keamanan tersebut yaitu:

1 Komunikasi yang jelas mengenai arti dan pentingnya sebuah kebijakan keamanan untuk disusun dan ditaati oleh seluruh pemangku kepentingan perusahaan;
2 Definisi yang jelas dan ringkas mengenai aset informasi apa saja yang harus diprioritaskan untuk dilindungi dan dikelola dengan sebaik-baiknya;
3 Penentuan ruang lingkup pemberlakukan kebijakan yang dimaksud dalam teritori kewenangan yang ada;
4 Jaminan adanya sanksi, perlindungan, dan penegakan hukum terhadap para pelaku yang terkait dengan manajemen informasi sesuai dengan peraturan dan undang-undang yang berlaku;
5 Adanya pembagian tugas dan tanggung jawab yang jelas terhadap personel atau SDM yang diberikan tugas untuk melakukan kegiatan pengamanan informasi;
6 Penyusunan dokumen atau referensi panduan bagi seluruh pemangku kepentingan dan pelaku manajemen keamanan informasi untuk menjamin penerapan yang efektif; dan
7 Partisipasi aktif dan intensif dari manajemen atau pimpinan puncak organisasi untuk mensosialisasikan dan mengawasi implementasi kebijakan dimaksud.

2.8 Model Pengembangan Kebijakan Keamanan Informasi

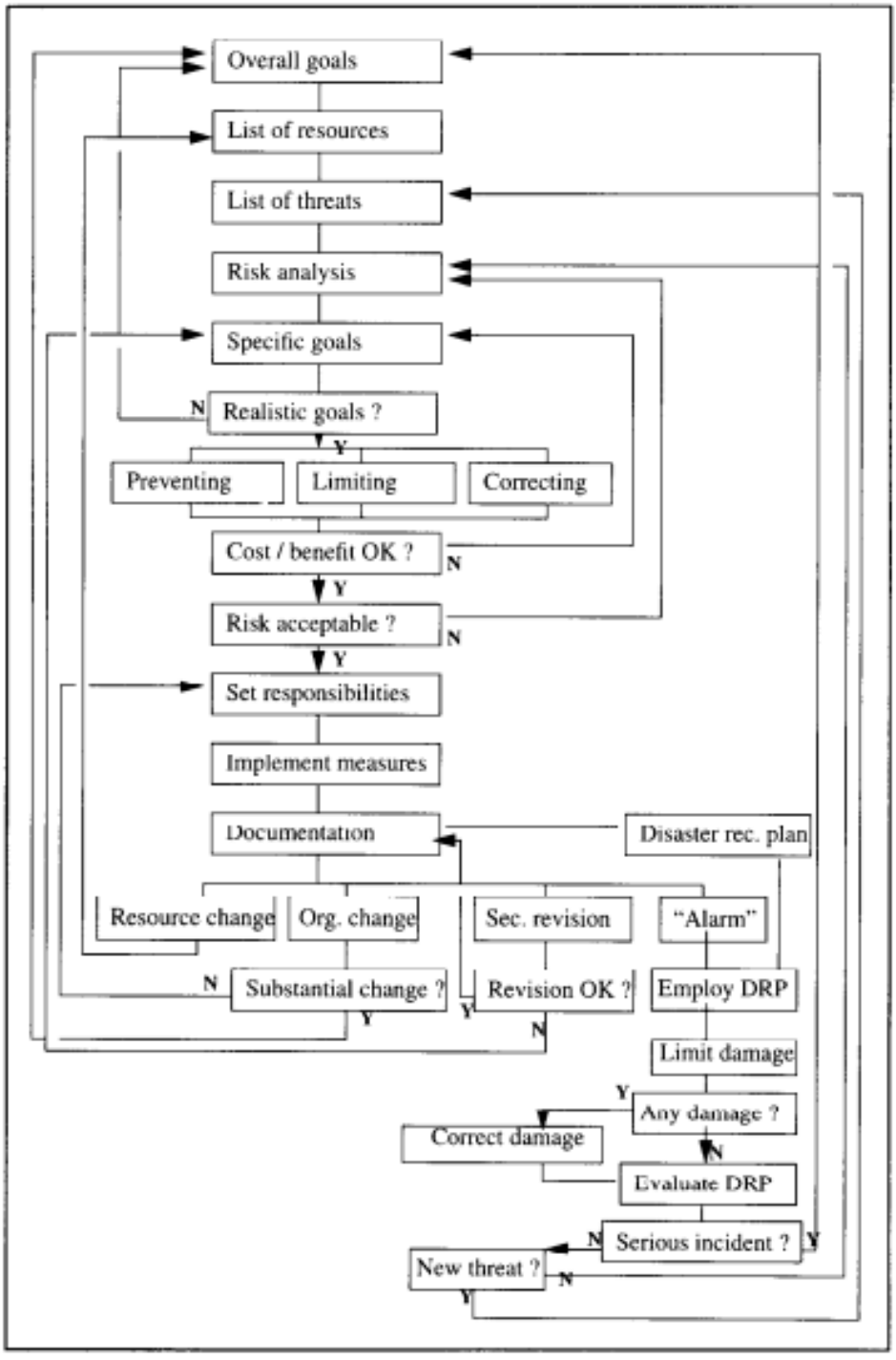
Di dalam membangun suatu kebijakan keamanan informasi pada organisasi, beberapa peneliti telah menawarkan konsep tentang bagaimana suatu kebijakan keamanan informasi dibangun dari awal sampai dengan dapat diimplementasikan serta di evaluasi oleh manajemen pada suatu organisasi.

2.8.1 Model penelitian Jon Olnes

Pada tahun 1994, Jon Olnes memberikan gambaran tentang bagaimana sebuah kebijakan keamanan informasi dikembangkan. Tahapan yang dikonsepkan oleh Olnes dimulai dengan penentuan tujuan umum dari kebijakan keamanan, lalu identifikasi sumber daya, selanjutnya identifikasi ancaman dan risiko, penentuan

tujuan khusus, penataan tanggungjawab, selanjutnya yaitu implementasi yang terukur dilanjutkan dengan pembuatan dokumentasi. (Ølnes, 1994)

Konsep kebijakan keamanan informasi yang digagas oleh Olnes tersebut dapat dilihat pada gambar dibawah ini:



Gambar 2.4 Methods for Security Policy yang dikonsep oleh Olnes (Ølnes, 1994)

2.8.2 Model Penelitian Jackie Ress

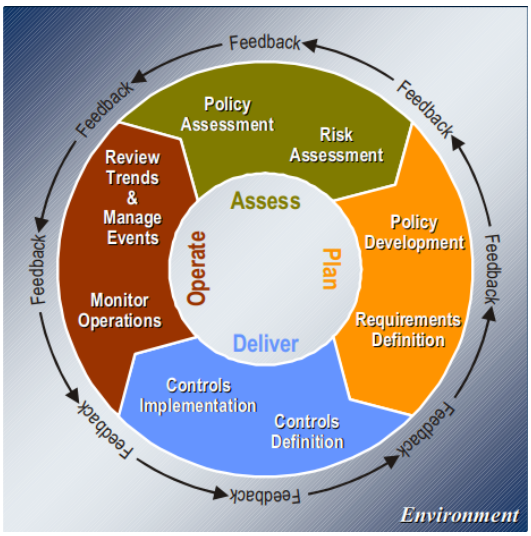
Jackie Ress Ulmer, pada penelitiannya di tahun 2003 menawarkan konsep "PFIRES: *Policy Framework for Interpreting Risk in e-Business Security*" dalam pengembangan kebijakan keamanan informasi. PFIRES dibangun dari berdasar siklus hidup pengembangan sistem (SDLC). Siklus PFIRES terdiri aras 4 (empat) fase utama yaitu : Penilaian (*Assess*), Perencanaan (*Plan*), Penyampaian (*Deliver*) dan Pengoperasian (*Operate*). Setiap fase didefinisikan dengan jelas dengan kriteria luaran tertentu yang harus dipenuhi sebelum berpindah ke fase berikutnya. (Ulmer et al., 2003)

Berikut adalah tabel fase dan sub-fase dari PFIRES Model.

Tabel 2.1 Fase dan sub-fase dari PFIRES Model

Fase	Sub-Fase
Assess	• Penilaian Kebijakan (lama) • Penilaian Risiko
Plan	• Pengembangan Kebijakan • Pendefinisian Kebutuhan
Deliver	• Pendefinisian Kontrol • Implementasi Kontrol
Operate	• Operasi Monitor • Tinjau ulang kecenderungan dan pengelolaan kegiatan.

Gambar dari siklus hidup PFIRES yang ditawarkan oleh Rees adalah sebagai berikut ini:



Gambar 2.5 Bagan Siklus Hidup PFIRES (Ulmer et al., 2003)

2.8.3 Model Penelitian Avinash W. Kadam

Pada tahun 2007, Kadam mempublikasikan penelitiannya terkait pengembangan kebijakan keamanan informasi. Menurut Kadam pengembangan kebijakan keamanan informasi adalah langkah yang sangat penting. Kredibilitas seluruh program keamanan informasi suatu organisasi tergantung pada kebijakan keamanan informasi yang dirancang dengan baik. (Kadam, 2007).

Walaupun Kadam tidak menggambarkan konsep pengembangan kebijakan keamanan informasi dalam bentuk diagram, tetapi beliau memberikan penjelasan secara rinci langkah pengembangan kebijakan tersebut. Adapun langkah dalam pengembangan kebijakan keamanan tersebut sebagai berikut:

- Kebijakan keamanan informasi level top manajemen.
  Hal ini terkait dengan gambaran komitmen dan tanggung jawab manajemen terhadap kebijakan keamanan informasi yang akan dikembangkan.
- Identifikasi ancaman
  Pada tahap ini dilakukan pendataan ancaman yang mungkin terjadi pada keamanan informasi. Baik itu ancaman dari dalam maupun ancaman dari luar organisasi.
- Penilaian kerentanan
  Tahapan ini memberikan penjelasan terhadap kerentanan dan risiko yang mungkin terjadi terhadap keamanan informasi.
- Identifikasi Perencanaan aksi
  Setelah risiko dan kerentanan terukur, maka langkah selanjutnya bagaimana rencana meminimalkan terjadi kerusakan atau kehilangan informasi.
- Menuliskan kebijakan keamanan informasi
  Penulisan kebijakan ini bertujuan agar kebijakan yang telah ditetapkan dapat terdokumentasi dan dapat dijadikan landasan hukum pelaksanaan program keamanan informasi.
- Implementasi Kebijakan
  Tahap selanjutnya yaitu bagaimana kebijakan keamanan yang telah ditetapkan dan terdokumentasikan dapat dilaksanakan dengan sungguh-sungguh, baik dari level top manajemen sampai dengan level operasional.

2.8.4 Model Penelitian Luay A. Wahsheh dan Jim Alves-Foss

Washeh dan Foss, pada tahun 2008 memberikan konsep daur hidup kebijakan dengan istilah RDIEE (*Requirements, Design, Implementation, Enforcement, and Enhancement*) dimana konsep yang ditawarkan tersebut dilakukan pengujian secara logis menggunakan bahasa pemrograman. (Wahsheh and Alves-Foss, 2008)

Adapun langkah pada tahapan RDIEE yang dikonsep oleh Washeh adalah sebagai berikut:

- *Policy requirements analysis*

  Pada tahap ini, kebutuhan bisnis dan batasan diidentifikasi. Deskripsi entitas, daerah rawan, dan tujuan kebijakan keamanan harus didefinisikan secara jelas.

- *Policy design*

  Pada tahap ini, dokumen persyaratan kebijakan ditinjau secara matang dan disesuaikan dengan kondisi yang akan diterapkan. Kebijakan level tinggi disempurnakan dan dijabarkan menjadi kebijakan level rendah

- *Policy implementation*

  Pada tahap ini, implementasi dimulai dengan dokumen desain kebijakan dan diujicobakan dengan kode dalam bahasa pemrograman.

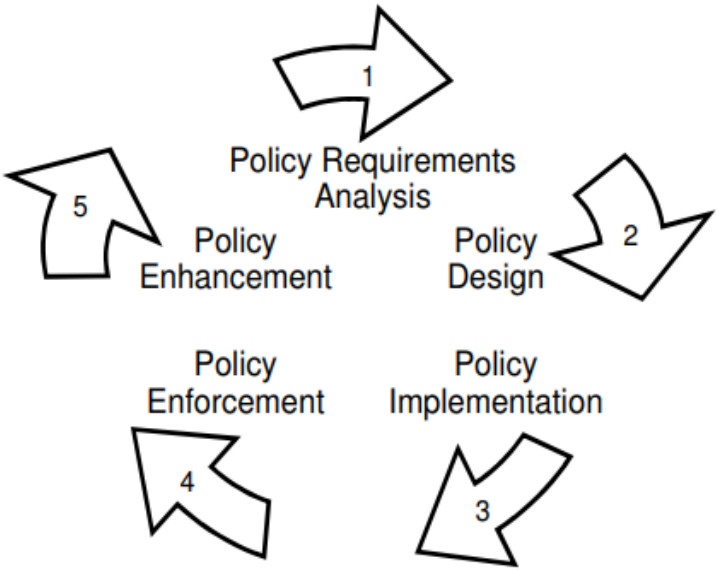
- *Policy enforcement*

  Pada tahap ini, dilakukan penegakan kebijakan dengan melakukan penjagaan komunikasi antar perangkat komunikasi jaringan seperti penetapan enkripsi pada komunikasi.

- *Policy enhancement*

  Pada tahap ini, sistem kebijakan keamanan berevolusi untuk memenuhi setiap perubahan dalam persyaratan kebijakan.

Konsep RDIEE yang dijelaskan oleh Wahsheh tersebut digambarkan dalam diagram dibawah ini:



Gambar 2.6 Siklus Hidup Kebijakan Keamanan RDIEE (Wahsheh and Alves-Foss, 2008)

2.8.5 Model Penelitian Kenneth J. Knapp , dkk.

Menurut Knapp pada penelitiannya yang dipublikasi tahun 2009, bahwa pengembangan kebijakan keamanan informasi pada organisasi dilakukan dengan melaksanakan 9 (sembilan) tahapan (Knapp et al., 2009). Adapun tahapan pengembangan kebijakan keamanan informasi yang dimaksud oleh Knapp yaitu:

1. Risk Assessment

2. Policy Development

3. Policy Approval

4. Policy Awareness & Training

5. Policy Implementation

6. Monitoring (Audits & Automated Tools)

7. Policy Enforcement

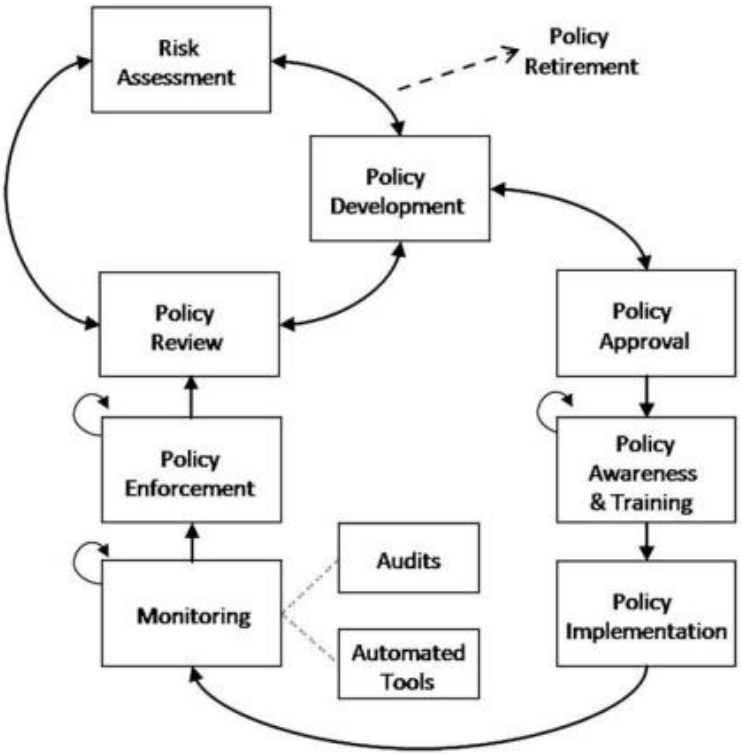
8. Policy Review

9. Policy Retirement

Semua tahapan harus dilakukan secara berurutan berkesinambungan. Dan untuk menjaga kualitas pada setiap tahapan, terkadang diperlukan proses peninjauan ulang pada setiap tahapan sebelum pindah ke tahap berikutnya. Kebijakan yang

telah dirancang sebelumnya wajib dilakukan peninjauan kembali sebagaimana kebutuhan dan kondisi perubahan pada organisasi.

Desain konsep pengembangan kebijakan keamanan informasi yang dipublikasikan oleh Knapp dapat dilihat pada gambar 2.7 dibawah ini.



Gambar 2.7 Model Kebijakan Keamanan Informasi sebagai proses yang berulang pada organisasi (Knapp et al., 2009)

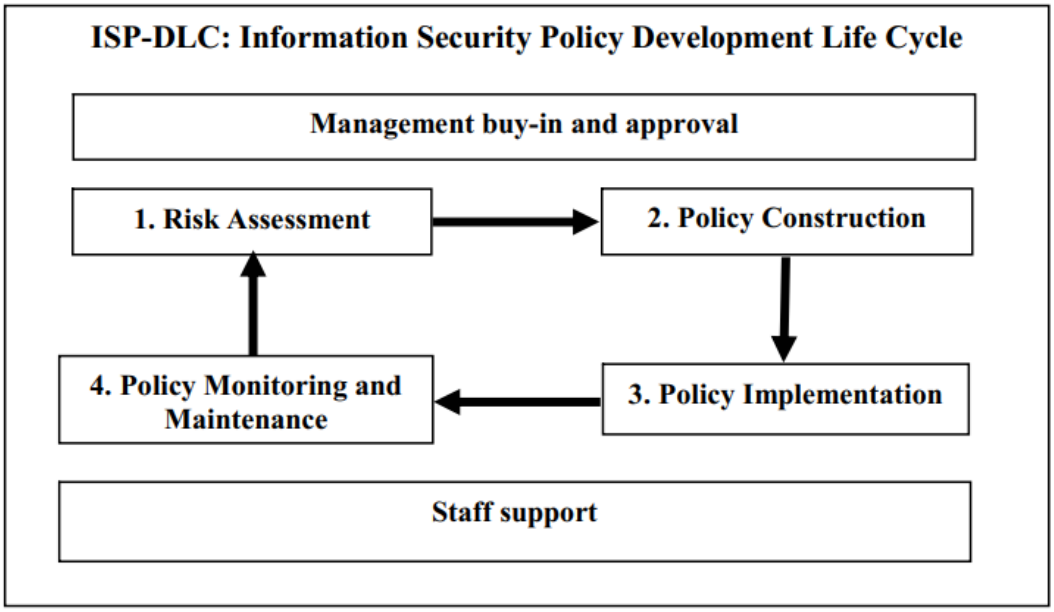
2.8.6 Model Penelitian T. Tuyikeze dan D. Pottas

Pada tahun 2011 Tuyikeze dan Pottas memberikan konsep daur hidup kebijakan keamanan informasi. Konsep yang ditawarkan oleh keduanya pun tidak berbeda jauh dengan apa yang telah dikonsepkan oleh peneliti sebelumnya. Perbedaan konsep yang ditawarkan hanya pada jumlah fase pengembangan kebijakan keamanan informasi yang dipersingkat menjadi 4 (empat) fase saja yaitu:

1. *Risk Assessment*
2. *Policy Construction*
3. *Policy Implementation*
4. *Policy Monitoring* dan *Maintenance*

Menurut Tuyikeze, setiap fase yang ada pada daur hidup kebijakan keamanan informasi dapat diperluas menjadi langkah-langkah kegiatan yang lebih terinci dan mendetail. Penting untuk diingat bahwa pengembangan kebijakan adalah proses berulang dan berkelanjutan. Karena perubahan teknologi, lingkungan bisnis dan persyaratan kepatuhan hukum, fase implementasi kebijakan akan selalu diikuti oleh fase pemeliharaan yang menggabungkan perubahan-perubahan ini dan fase pemantauan yang memastikan bahwa arahan kebijakan dijalankan secara operasional (yaitu kepatuhan kebijakan). (Tuyikeze and Pottas, 2011)

Diagram daur hidup kebijakan keamanan informasi yang dikonsep oleh Tuyikeze dapat dilihat pada gambar 2.8 berikut ini:



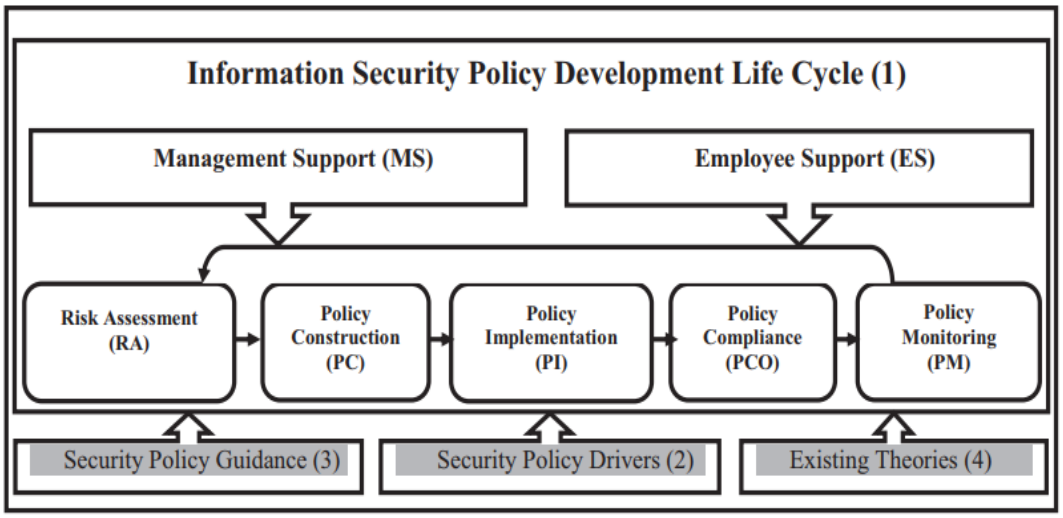
Gambar 2.8 Model ISP-DLC (Tuyikeze and Pottas, 2011)

2.8.7 Model Penelitian Stephen V. Flowerday dan Tite Tuyikeze

Pada penelitian yang dilakukan oleh Flowerday dan Tuyikeze yang dipublikasikan pada tahun 2016 ini, merupakan penyempurnaan dari konsep yang ditawarkan oleh Tuyikeze sebelumnya. Pada penelitian ini melibatkan 7 (tujuh) elemen pembangun. Tujuh konstruksi komponen ISPDLC, yaitu *Risk Assessment* (RA), *Policy Construction* (PC), *Policy Implementation* (PI), *Policy Compliance* (PCO), *Policy Monitoring* (PM), *Management Support* (MS) dan *Employee Support* (ES) dimana semua telah dievaluasi berdasarkan hasil survei.

Dari hasil tes analis yang dilakukan menunjukkan bahwa dukungan dari manajemen dan dukungan dari pegawai sangat perlu. Hal ini menunjukkan peran dari manajemen dan pegawai di dalam proses daur hidup pengembangan kebijakan keamanan informasi. Selain itu, hasil dari analisis menunjukkan ke-7 elemen pembangun memiliki hubungan korelasi positif serta dapat diandalkan dan konsisten. (Flowerday and Tuyikeze, 2016).

Diagram daur hidup kebijakan keamanan informasi yang dikonsep oleh Flowerday dapat dilihat pada gambar 2.9 berikut ini:



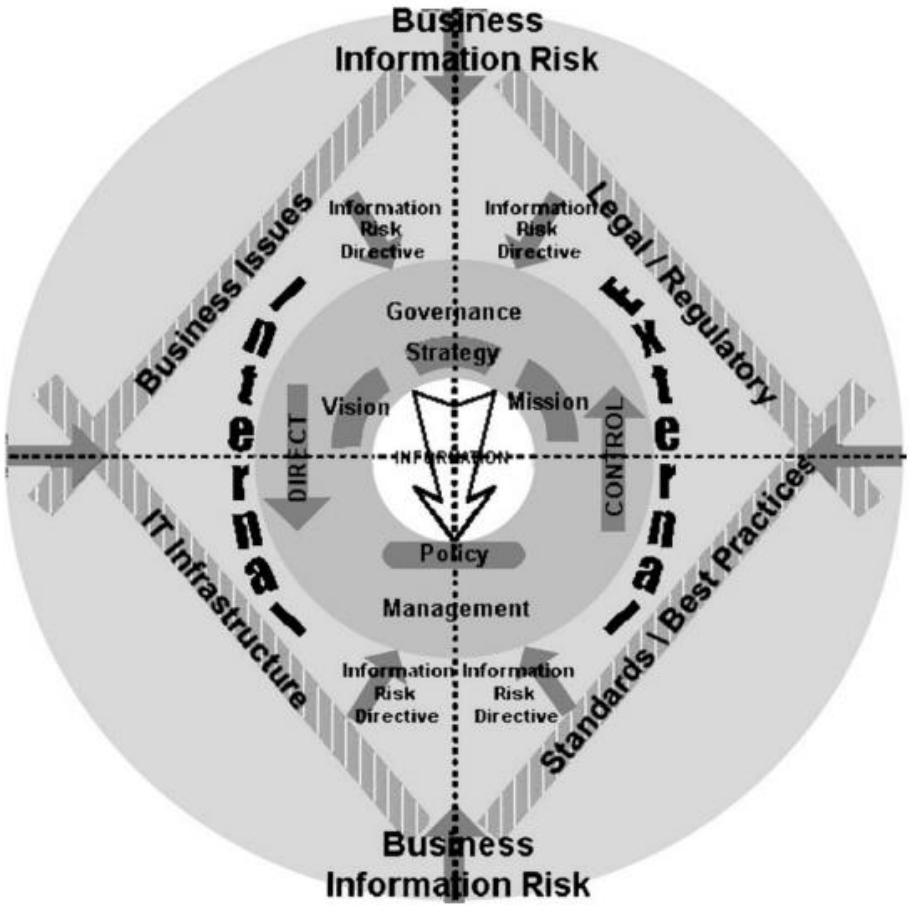
Gambar 2.9 Model ISPDLC 7 elemen (Flowerday and Tuyikeze, 2016).

2.9. Hubungan Kebijakan Keamanan Informasi dan Strategi Organisasi

Berdasar model atau kerangka kerja pengembangan kebijakan keamanan informasi yang telah dijelaskan oleh para peneliti sebelumnya, tidak ada yang menyebutkan bahwa di dalam pengembangan kebijakan keamanan informasi haruslah mempertimbangkan strategi organisasi khususnya strategi keamanan informasi. Padahal kebijakan keamanan informasi merupakan bagian vital dari strategi organisasi demi tercapainya keamanan informasi. (Höne and Eloff, 2002).

Sedangkan menurut Whitman yang dikutip oleh Posthumus, menyebutkan bahwa dalam mencapai keamanan informasi pada organisasi, manajemen level atas berkewajiban membentuk kebijakan keamanan informasi organisasi untuk menunjukkan komitmen mereka atas keamanan informasi, visi, misi dan strategi organisasi. Lebih lanjut Posthumus menjelaskan bahwa dalam kerangka kerja tata

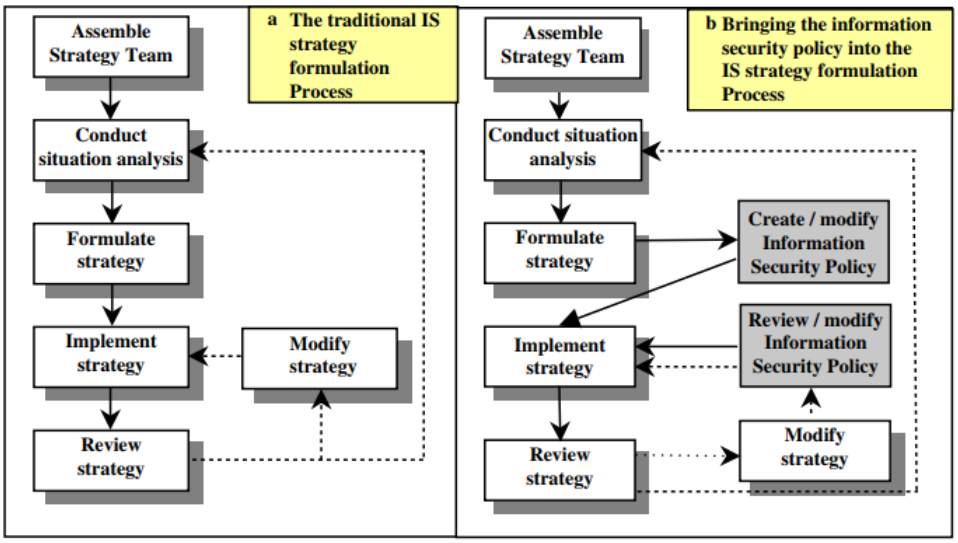
kelola keamanan informasi, kebijakan keamanan merupakan perwujudan terlaksanakannya visi, misi dan strategi organisasi. (Posthumus and von Solms, 2004). Konsep kerangka kerja tata kelola keamanan informasi yang dijelaskan oleh Posthumus terlihat pada gambar dibawah ini:



Gambar 2.10 Kerangka kerja tata kelola keamanan informasi (Posthumus and von Solms, 2004)

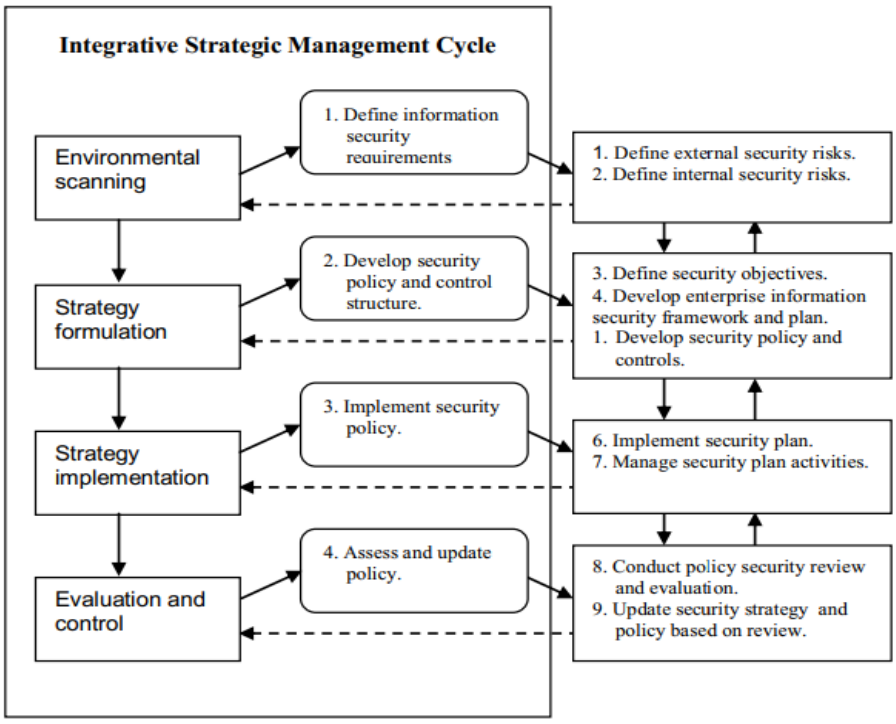
Sejalan dengan pemikiran Posthumus, Doherty menjelaskan bahwa di dalam mengembangkan kebijakan keamanan informasi haruslah selaras dengan strategi keamanan informasi pada organisasi. Artinya jika strategi keamanan informasi dilakukan perubahan maka kebijakan keamanan informasi yang ada pun harus ikut diubah dengan mengikuti strategi yang dibuat, jangan sampai kebijakan keamanan yang telah ada bertentangan dengan strategi keamanan yang dibuat. (Doherty and Fulford, 2006).

Gambar diagram konsep pengembangan rencana strategi sistem informasi yang dijelaskan oleh Doherty dapat dilihat pada gambar dibawah ini:



Gambar 2.11 Pengembangan rencana strategi sistem informasi (SISP) (Doherty and Fulford, 2006)

Konsep yang menyebutkan bahwa dalam pengembangan kebijakan informasi harus dilandasi oleh strategi organisasi juga disetujui oleh Maria Soto. Soto menyebutkan bahwa kebijakan keamanan informasi merupakan dasar kebijakan strategi bisnis dalam perencanaan strategi organisasi. (Soto, 2011) Konsep tersebut tergambar dalam bagan berikut ini:



Gambar 2.12 Pendekatan terintegrasi dalam pengembangan kebijakan keamanan informasi (Soto, 2011)

2.10 Sistem Manajemen Keamanan Informasi (SMKI) pada Perguruan Tinggi

Seiring dengan perkembangan dan pemakaian teknologi informasi di lingkungan perguruan tinggi di Indonesia, maka tata kelola dan manajemen keamanan informasi pun tak elak harus diterapkan di lingkungan perguruan tinggi. Untuk itu beberapa penelitian terkait Manajemen Keamanan Informasi pada perguruan tinggi juga dilakukan.

Penelitian yang dilakukan oleh Cheung (Cheung, 2014) menyebutkan bahwa keamanan informasi sangat penting bagi lembaga pendidikan tinggi karena kebocoran dan kerusakan informasi akan menimbulkan kerugian besar. Ada kebutuhan untuk lembaga pendidikan tinggi untuk menegakkan keamanan informasi. Berdasarkan prinsip-prinsip keamanan informasi, terdapat delapan area kontrol pada keamanan informasi, yaitu, kontrol aset informasi, kontrol personel, kontrol fisik, kontrol akses, kontrol komunikasi, kontrol operasi, kontrol sistem informasi, dan manajemen insiden dan kontinuitas bisnis. Kebijakan, pedoman, dan langkah-langkah pengendalian harus ditetapkan. Sementara kebijakan memberikan aturan tata kelola keamanan informasi, pedoman dan langkah-langkah kontrol membantu melaksanakan dan menerapkan kebijakan. Namun demikian dukungan dari manajemen tingkat atas sangat diperlukan.

Sedangkan Ghazvini dkk menyebutkan kebijakan keamanan informasi tidak mudah dikembangkan kecuali organisasi secara jelas mengidentifikasi langkah-langkah yang diperlukan dalam proses pengembangan kebijakan keamanan informasi, khususnya di lembaga-lembaga pendidikan tinggi yang sebagian besar memanfaatkan TI. Proses pengembangan yang tidak tepat atau replikasi konten kebijakan keamanan dari organisasi lain bisa gagal dalam eksekusi. Pelaksanaan kebijakan duplikat bisa gagal untuk bertindak sesuai dengan aturan dan peraturan yang dapat ditegakkan meskipun itu dikembangkan dengan baik. Tantangan bagi lembaga pendidikan tinggi adalah untuk memahami bagaimana mengembangkan dan menerapkan kebijakan keamanan informasi secara efektif berdasarkan analisis risiko sesuai dengan persyaratan organisasi. Kalau tidak, dalam kasus pelanggaran keamanan atau pelanggaran, kecil kemungkinannya untuk menegakkan peraturan

karena dokumen kebijakan keamanan yang tidak lengkap atau tidak dapat dipahami (Ghazvini et al., 2018).

Menurut penelitian Sari dkk, implementasi manajemen keamanan informasi yang dilakukan khususnya pada perguruan tinggi dimana mengambil studi kasus lembaga pendidikan tinggi di kota Bandung, menyebutkan dari 5 variabel pendukung manajemen keamanan informasi dikelompokkan menjadi 2 faktor, yaitu faktor 1 (variabel yang dominan) dan faktor 2 (variabel yang tidak dominan. Dari penelitian tersebut dapat disimpulkan bahwa menjadi faktor dominan pada pengembangan manajemen keamanan informasi pada perguruan tinggi yaitu variabel kesadaran, anggaran, kebijakan keamanan informasi, dan dukungan manajemen puncak. Sedangkan variabel Misi organisasi menjadi Faktor 2 dan faktor ini hanya memiliki pengaruh yang sangat kecil pada implementasi manajemen keamanan informasi. Yang berarti semakin lembaga pendidikan tinggi memperhatikan kesadaran, anggaran, kebijakan keamanan informasi, dan dukungan manajemen puncak, maka semakin sukses penerapan manajemen keamanan informasi (Sari and Nurshabrina, 2016).

Yustanti (Yustanti et al., 2018) pada penelitiannya yang berfokus pada analisis indeks keamanan informasi yang mengambil kasus pada universitas negeri di surabaya menyimpulkan:

1. Keamanan informasi telah dilaksanakan meskipun sebagian besar masih dalam bidang teknis dan tidak ada keterkaitan langkah-langkah keamanan untuk mendapatkan strategi yang efektif.
2. Proses keamanan informasi berjalan tanpa dokumentasi atau rekaman resmi.
3. Tindakan pengamanan operasional yang diterapkan tergantung pada pengetahuan dan motivasi individu pelaksana.
4. Keseluruhan bentuk pengamanan informasi belum terbukti efektivitasnya.
5. Kelemahan dalam manajemen keamanan informasi masih banyak ditemukan dan tidak dapat diselesaikan secara menyeluruh oleh pelaksana dan pemimpin yang menyebabkan dampak yang sangat signifikan.
6. Manajemen keamanan informasi belum diprioritaskan dan tidak berjalan secara konsisten.

2.11 Standar Keamanan Informasi ISO 27001:2013

Standar ISO didesain agar dapat digunakan oleh perusahaan pada semua sektor industri. Perusahaan besar, menengah, maupun kecil sekalipun dapat mengimplementasikan standar ini. ISO 27001 adalah sebuah metode khusus yang terstruktur yang mengatur mengenai cara pengamanan informasi yang diakui secara internasional dan nasional. ISO 27001 merupakan salah satu metode SMKI yang sangat populer dan diakui di banyak perusahaan. ISO 27001 memberikan gambaran umum mengenai apa saja yang harus dilakukan oleh sebuah perusahaan dalam usahanya untuk mengevaluasi, mengimplementasikan, dan memelihara keamanan informasinya di sebuah perusahaan berdasarkan *Best Practice* dalam pengamanan informasi.

Standar ISO 27001 merupakan bagian pertama dari kelompok standar mengenai sistem manajemen keamanan informasi. ISO 27001 berisi spesifikasi dari standar ISO 27000 yang dapat diaudit dan dapat disertifikasi. Secara umum standar ini merupakan sebuah kerangka kerja untuk membuat mengimplementasikan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan kinerja sistem manajemen keamanan informasi.

ISO 27001 merupakan standar sistem manajemen dan bukan merupakan standar teknik. ISO 27001 merupakan standar yang lebih mengatur secara manajemen dan bukan secara teknis karena keamanan informasi merupakan tanggung jawab manajemen secara bersama-sama bukan hanya merupakan tanggung jawab orang per orang. Aspek teknis diberikan secara tidak langsung karena lebih bersifat konseptual, sehingga penerapannya dapat disesuaikan dengan karakteristik berbagai perusahaan.

ISO 27001 mengikuti proses Plan Do Check Act atau sering disebut PDCA yang sesuai dengan proses SMKI pada umumnya yang dapat dilihat pada gambar 2.13 dibawah. Proses PDCA dijelaskan sebagai berikut :

1. *PLAN* (Perencanaan)

   Pada proses ini akan dilakukan beberapa langkah sebagai berikut :

   - Mendefinisikan tujuan bisnis
   - Mendapatkan dukungan dari manajemen

- Menentukan ruang lingkup dan tujuan pengamanan
- Mendefinisikan metode penilaian risiko
- Melakukan klasifikasi aset sesuai dengan klasifikasi risiko berdasarkan hasil penilaian risiko

2. *DO* (Pelaksanaan)

   Pada proses ini akan dilakukan beberapa langkah seperti dibawah ini :

   - Pengelolaan risiko dan membuat rencana mitigasi risiko
   - Menentukan kebijakan dan prosedur untuk mengontrol risiko
   - Mengalokasikan sumber daya dan memberikan pelatihan kepada karyawan

3. *CHECK* (Pengontrolan)

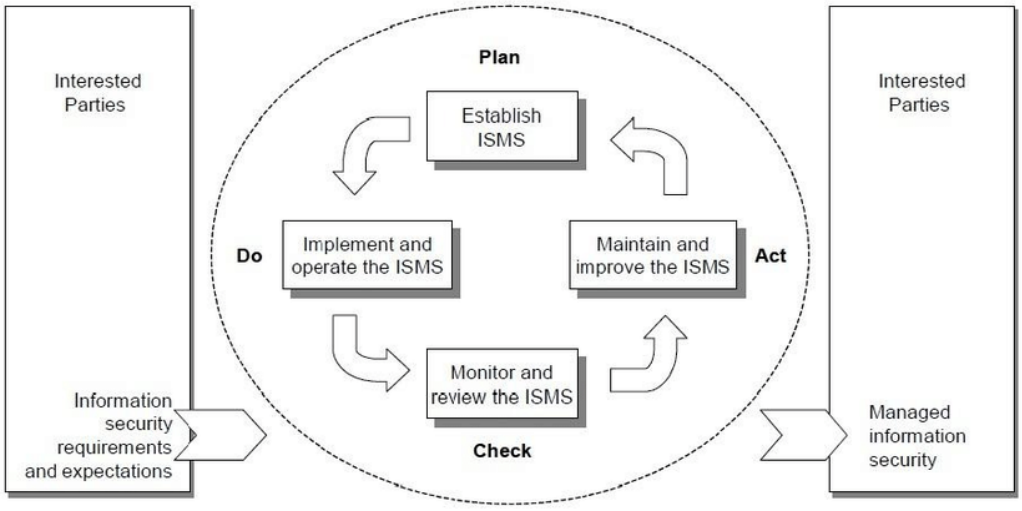
   Pada proses ini akan dilakukan beberapa langkah sebagai berikut :

   - Memonitor tingkat efektivitas SMKI
   - Internal audit, pra audit, dan audit sertifikasi untuk memperoleh sertifikat

4. *ACT* (Tindak Lanjut)

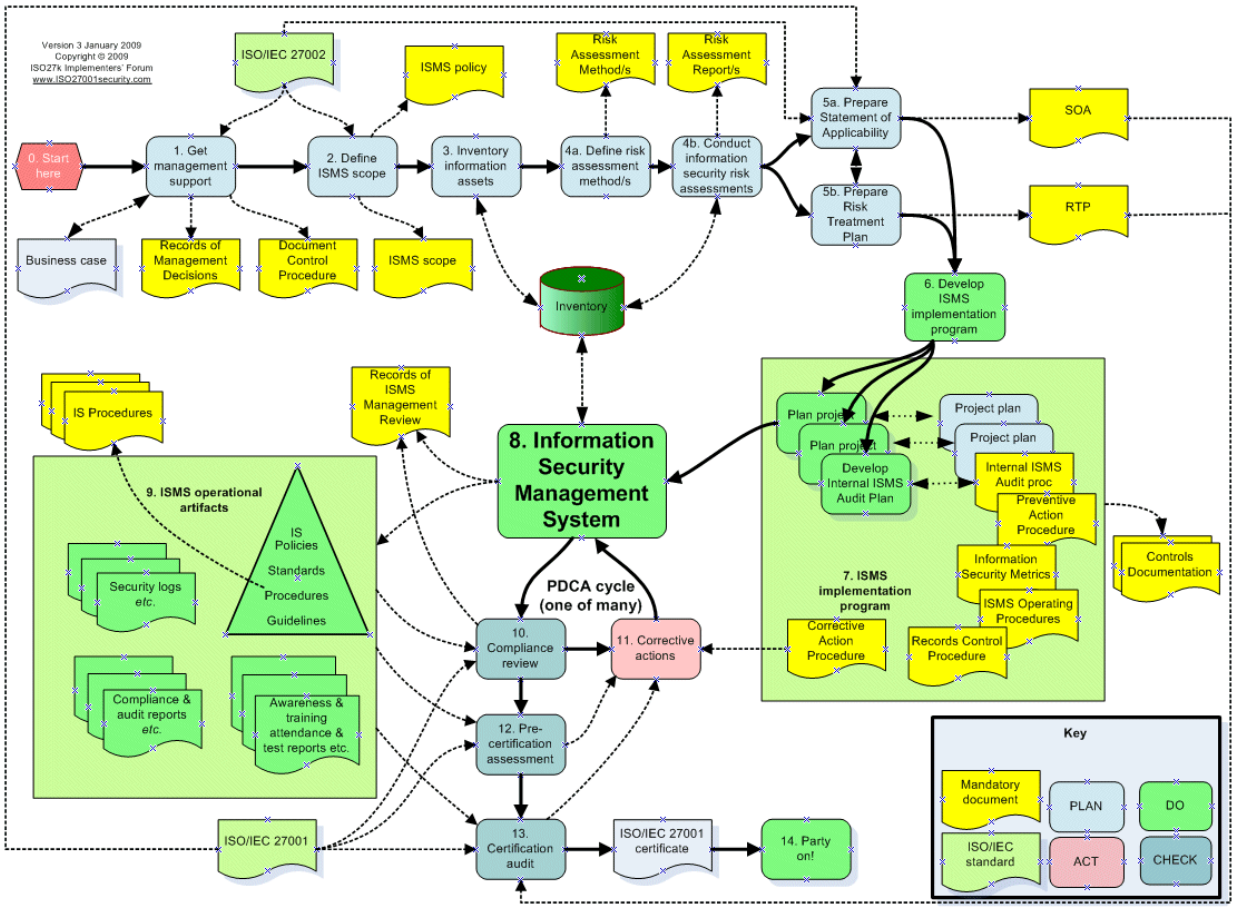
   Pada proses ini akan dilakukan beberapa langkah seperti dibawah ini :

   - Tindakan pencegahan dan perbaikan terhadap SMKI secara berkala
   - Meningkatkan proses SMKI secara terus-menerus agar lebih baik



Gambar 2.13 Siklus PDCA ISO 27001 (ISO27001, 2013)

ISO 27001 menerangkan bahwa hal yang paling penting dalam implementasi SMKI adalah komitmen manajemen untuk mendukung proses implementasi SMKI yang dapat dilihat pada gambar 2.14. Komitmen manajemen sangat penting karena pengamanan informasi merupakan masalah bisnis. Pengamanan informasi agar berjalan efektif menuntut keterlibatan manajemen puncak secara aktif untuk menilai ancaman yang makin meningkat setiap saat. Manajemen puncak dituntut untuk dapat melakukan respon ancaman yang timbul tersebut, sehingga keterlibatan manajemen puncak menjadi sangat penting dalam mendukung pelaksanaan SMKI. Manajemen berfungsi erat dengan tanggung jawab dan pengelolaan sumber daya manusia sehingga mampu mendukung keberlangsungan bisnis perusahaannya.



Gambar 2.14 Implementasi SMKI dengan Standar ISO 27001 (ISO27001, 2013)

Pada standar ISO 27001:2013 yang merupakan revisi dari ISO 27001:2005 memiliki 14 grub kontrol keamanan informasi yang berfungsi untuk menjaga terjaminnya keamanan informasi pada organisasi. Grup kontrol ISO 27001:2013 dijelaskan sebagai berikut :

1. Kebijakan Keamanan Informasi

   Grup kontrol ini membahas mengenai cara membuat kebijakan dan peninjauan kembali kebijakan tersebut dalam jangka waktu tertentu. Kebijakan akan mengalami perubahan seiring perjalanan waktu yang mengikuti dengan ancaman-ancaman baru yang timbul.

2. Keamanan Informasi Organisasi

   Grup kontrol ini mengatur mengenai pengelolaan keamanan informasi di dalam sebuah organisasi. Di dalam Grup kontrol ini diatur mengenai identifikasi peran dan tanggung jawab dan pemisahan tugas. Grup kontrol ini juga mengatur mengenai penggunaan perangkat *mobile* dan *teleworking*.

3. Keamanan Sumber Daya Manusia

   Grup kontrol ini mengatur mengenai manajemen pengelolaan sumber daya manusia mulai dari proses perekrutan, saat menjadi karyawan, dan pada saat pemberhentian karyawan. Manusia merupakan suatu ancaman terbesar sehingga sangat penting adanya kontrol dalam pengelolaannya.

4. Pengelolaan Aset

   Dalam grup kontrol ini berhubungan dengan manajemen aset perusahaan dan penggunaannya yang sesuai dengan tujuan perusahaan. Selain itu grup kontrol ini juga mengatur mengenai penanganan media dan pengklasifikasian aset sesuai dengan tingkat kepentingannya terhadap kinerja perusahaan.

5. Akses Kontrol

   Pengelolaan dan pengendalian akses informasi organisasi diatur dalam grup kontrol ini. Grup kontrol ini mengatur mengenai kebijakan akses kontrol, manajemen hak akses pengguna, akses kontrol terhadap sistem dan aplikasi, dan mengatur tanggung jawab pengguna.

6. Kriptografi

   Kriptografi mengatur mengenai kontrol terhadap enkripsi dan manajemen kunci agar informasi penting organisasi dapat dilindungi dari pencurian.

7. Keamanan Fisik dan Lingkungan

   Grup kontrol ini mengatur mengenai kontrol-kontrol yang perlu dilakukan terhadap keamanan secara fisik dan dari gangguan lingkungan. Kontrol yang berlaku mengenai pengamanan area, kontrol masuk, perlindungan terhadap ancaman, keamanan peralatan, dan lain sebagainya.

8. Operasi Keamanan

   Operasi keamanan mengatur mengenai pengelolaan dan pengendalian semua keamanan informasi, termasuk di dalamnya berupa prosedur operasional, tanggung jawab , audit, pengawasan, manajemen kerentanan teknis dan sistem informasi yang bersifat kritikal bagi organisasi.

9. Komunikasi Keamanan

   Grup kontrol ini membahas mengenai keamanan jaringan, transfer informasi dan lain sebagainya. Fokus utamanya adalah mengamankan jaringan secara fisik dan layanan yang digunakannya.

10. Akuisisi Sistem, pengembangan, dan Pemeliharaan

    Dalam grup kontrol ini diuraikan mengenai cara pengelolaan pengelolaan keamanan menyangkut proses pengembangan sistem dan pemeliharaannya.

11. Hubungan dengan pemasok

    Grup kontrol ini mengatur tata cara pengelolaan keamanan yang berhubungan dengan pemasok. Diperlukan mekanisme untuk mengontrol pemasok dan prosedur perjanjian kerja dengan pemasok.

12. Manajemen Insiden Keamanan Informasi

    Grup kontrol ini mengatur mengenai tata cara penanganan jika terjadi insiden terhadap keamanan informasi. Di dalam manajemen insiden harus ada kontrol mengenai pelaporan insiden, mendefinisikan tanggung jawab, prosedur respon terhadap insiden, dan pengumpulan bukti untuk pelaporan.

13. Aspek Keamanan Informasi dari Manajemen Keberlangsungan Bisnis

    Keberlangsungan bisnis diatur dalam grup kontrol ini. Kontrol di dalamnya meliputi perencanaan manajemen keberlangsungan bisnis, prosedur, verifikasi, pengembangan, dan redudansinya.

14. Kepatuhan

Grup kontrol terakhir ini mengatur mengenai kepatuhan organisasi terhadap persyaratan hukum yang berlaku. Di dalamnya terdapat mengenai kepatuhan terhadap perlindungan data pribadi, perlindungan kekayaan intelektual dan lain sebagainya.

Pada Tabel 2.2 berikut dijelaskan grup kontrol dan sasaran kontrol dari kerangka kerja ISO 27001:2013, dimana terdapat 14 grup kontrol ISO 27001:2013 dan 35 buah sasaran pengendaliannya.

Tabel 2.2 Grup kontrol ISO 27001:2013 dan sasaran pengendaliannya.

Grup Kontrol		**Sasaran Pengendalian**	
1	*Information security policies*	1	*Management direction for information security*
2	*Organization of information security*	2	*Internal organization*
		3	*Mobile device and teleworking*
3	*Human resouces security*	4	*Prior to employment*
		5	*During employment*
		6	*Termination and change of employment*
4	*Asset management*	7	*Responsibility for assets*
		8	*Information classification*
		9	*Media handling*
5	*Access control*	10	*Bussiness requirements for access control*
		11	*User access management*
		12	*User responsibilities*
		13	*System and applicaiton access control*
6	*Cryptography*	14	*Cryptographic controls*
7	*Physical and environmental security*	15	*Secure area*
		16	*Equipment*
8	*Operations security*	17	*Operational procedures and responsibilities*
		18	*Protection from malware*
		19	*Backup*
		20	*Logging and monitoring*
		21	*Control of operational software*
		22	*Technical vulnerabilities management*

Grup Kontrol		Sasaran Pengendalian	
		23	*Information systems audit consierations*
9	*Communications security*	24	*Network security management*
		25	*Information transfer*
10	*System acquisition, development and maintenance*	26	*Security requirements of information system*
		27	*Security in development and support processes*
		28	*Test data*
11	*Supplier relationship*	29	*Information security in supplier relationship*
		30	*Supplier service delivery management*
12	*Infomation security incident management*	31	*Management of information security incidents and improvements*
13	*Information security aspects of bussiness continuity management*	32	*Information security continuity*
		33	*Redundancies*
14	*Compliance*	34	*Compliance with legal and contractual requirement*
		35	*Information security reviews*

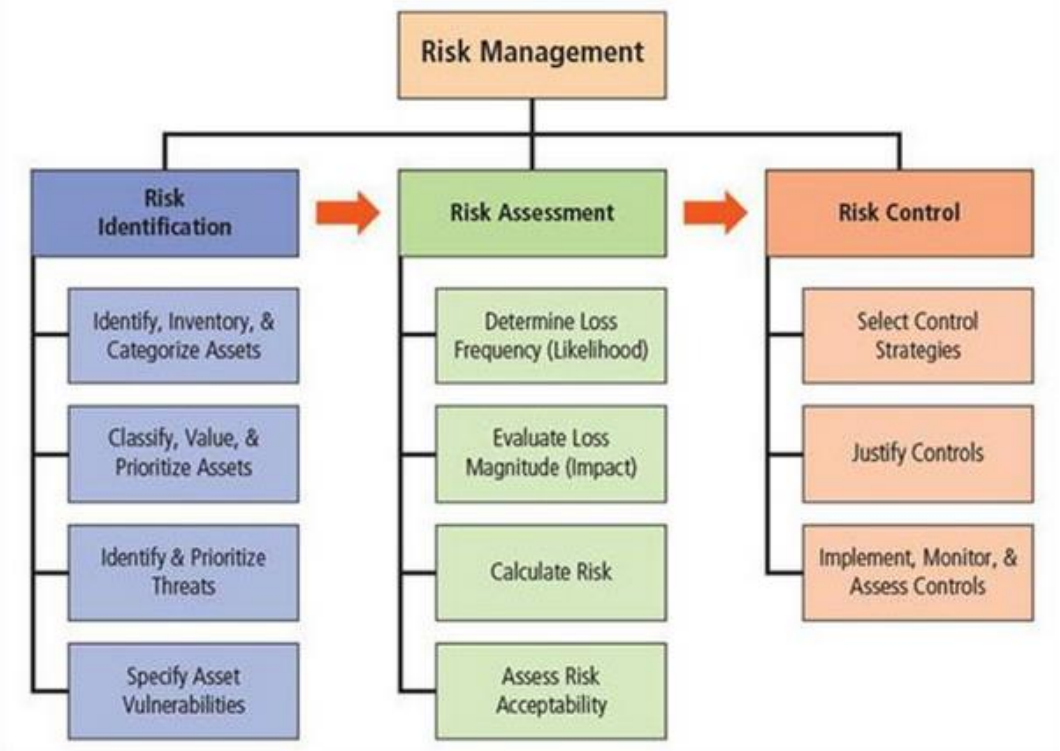
Adapun penjelasan untuk tiap-tiap kontrol yang ada pada ISO 27001:2013, dapat lihat pada Lampiran A.

2.12 Penilaian Risiko Keamanan Informasi

Penilaian risiko merupakan langkah yang paling penting pada awal proyek keamanan informasi organisasi, dalam hal ini adalah menetapkan dasar-dasar untuk keamanan informasi di organisasi. penilaian risiko merupakan suatu aktivitas yang dilaksanakan untuk memperkirakan suatu risiko dari situasi yang bisa didefinisikan dengan jelas ataupun potensi dari suatu ancaman atau bahaya baik secara kuantitatif atau kualitatif. Penilaian risiko juga bisa diartikan sebagai suatu proses pemeriksaan keamanan dengan suatu struktur tertentu, pembuatan suatu rekomendasi khusus, dan rekomendasi pengambilan keputusan dalam suatu proyek dengan menggunakan analisis risiko, perkiraan risiko, dan informasi lain yang memiliki potensi untuk mempengaruhi keputusan.

Di dalam melakukan penilaian risiko keamanan informasi memang tidak membutuhkan usaha yang sedikit, maksudnya banyak hal yang harus dipersiapkan dan dilakukan agar proses penilaian risiko dapat berjalan dengan sebenarnya dan mendapatkan hasil penilaian yang optimal sehingga manajemen organisasi benar-benar mengerti akan risiko yang dihadapi oleh organisasi sehingga dapat mengambil keputusan penerimaan risiko keamanan informasi organisasi sesuai dengan keadaan dan kemampuan organisasi.

Pada gambar 2.15 dibawah, dijelaskan komponen atau aktivitas apa saja yang harus dilakukan dalam upaya pengelolaan risiko keamanan informasi yang sesungguhnya.



Gambar 2.15 Komponen Manajemen Risiko Keamanan Informasi (Cengage Learning, 2018)

Adapun detail langkah penilaian risiko keamanan informasi sebagaimana ditulis oleh Riyanarto Sarno, dll pada bukunya yang berjudul "Sistem Manajemen Keamanan Informasi Berbasis ISO 27001" (Sarno and Iffano, 2009), adalah sebagai berikut:

2.12.1 Identifikasi Aset dan Penilaian Aset

Proses identifikasi Aset yaitu proses identifikasi jenis aset yang dimiliki oleh organisasi, baik aset informasi maupun aset pendukung informasi ataupun aset non informasi. Selanjutnya diklasifikasikan berdasar macam jenis aset informasi, seperti database, sistem informasi, perangkat lunak, perangkat keras, jaringan komputer, manusia dan sebagainya. Pada proses ini perlu dilakukan pendataan yang detail terkait masing-masing aset, baik spesifikasi aset, tahun pengadaan, lokasi, fungsi, pengelola dan yang lainnya.

Hasil dari proses identifikasi aset ini dipaparkan dalam bentuk tabel inventaris aset dengan format yang mudah untuk dibaca dan dipahami oleh semua pihak yang selanjutnya akan digunakan sebagai bahan untuk menghitung nilai aset.

Menghitung nilai aset adalah menghitung nilai informasi yang dimiliki oleh organisasi. Dimana aset yang dihitung hanya informasi dan aset yang termasuk dalam ruang lingkup Sistem Manajemen Keamanan Informasi yang telah didefinisikan sebelumnya. Cara menghitung nilai aset dapat didasarkan aspek dasar keamanan informasi yaitu kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*).

Berikut adalah tabel 2.3 yang memberikan gambaran penilaian aset berdasar kriteria kerahasiaan (*confidentiality*).

Tabel 2.3 Penilaian aset berdasar kriteria kerahasiaan (confidentiality)

Kriteria *Confidentiality*	**Nilai *Confidentiality* (NC)**
Public	0
Internal use only	1
Private	2
Confidential	3
Secret	4

Sumber : (Sarno and Iffano, 2009)

Keterangan:

Public = Informasi / aset tidak ada yang rahasia dan bisa diakses oleh umum.

Internal use only = informasi / aset yang ada hanya diperbolehkan diakses oleh internal organisasi.

Private = Informasi / aset hanya boleh diakses oleh unit/departemen tertentu dalam organisasi.

Confidential = informasi / aset hanya boleh diakses oleh sub unit/ sub departemen dalam suatu unit/departemen.

Secret = informasi / aset hanya boleh diakses oleh personal/tim/manajemen tertentu.

Adapun gambaran penilaian aset dengan dasar integritas *(integrity)* dapat dilihat pada tabel 2.4 berikut.

Tabel 2.4 Penilaian aset berdasar kriteria integritas (integrity)

Kriteria *Integrity*	**Nilai *Integrity* (NI)**
No Impact	0
Minor incident	1
General disturbance	2
Mayor disturbance	3
Unacceptable damage	4

Sumber : (Sarno and Iffano, 2009)

Keterangan:

No Impact = Kerusakan data / aset tidak berpengaruh

Minor incident = toleransi kerusakan informasi / aset max 25%

General disturbance = toleransi kerusakan informasi / aset max 15%

Mayor disturbance = toleransi kerusakan informasi / aset max 10%

Unacceptable damage = tidak ada toleransi kerusakan informasi / aset (100% benar/prima)

Sedangkan gambaran tentang penilaian aset berdasar kriteria Ketersediaan *(Availability)* dipaparkan pada tabel 2.5 berikut:

Tabel 2.5 Penilaian aset berdasar kriteria Ketersediaan (Availability)

Kriteria *Availability*	**Nilai *Availability* (NA)**
Low / No Availability	0
Office hours Availability	1
Strong Availability	2
High Availability	3
Very High Availability	4

Sumber : (Sarno and Iffano, 2009)

Keterangan:

Low / No Availability = informasi / aset boleh tidak ada

Office hours Availability = informasi / aset hanya bisa tersedia pada jam kantor

Strong Availability = informasi / aset boleh tidak tersedia max. 24 Jam (Toleransi kerusakan 1 hari)

High Availability = informasi / aset boleh tidak tersedia max. 12 Jam (Toleransi kerusakan 0,5 hari)

Very High Availability = informasi / aset harus selalu ada.

Selanjutnya dari ketiga tabel diatas dilakukanlah perhitungan nilai aset (*Asset value*), yaitu dengan menggunakan persamaan matematis berikut:

Nilai Aset (NA) = NC + NI + NV

Dimana:

NA = Nilai Aset yang didapatkan

NC = Nilai *Confidentiality* sesuai dengan nilai yang ada ditabel

NI = Nilai *Integrity* sesuai dengan nilai yang ada ditabel

NV = Nilai *Availability* sesuai dengan nilai yang ada ditabel

Contoh dari penggunaan persamaan matematika untuk menentukan Nilai Aset tersebut adalah sebagai berikut:

Jenis Aset : Data / Sistem Informasi

Nama Aset : SIM Akademik

Nilai Aset :

- Nilai *Confidentiality* yang diperoleh (NC = 3)
- Nilai *Integrity* yang diperoleh (NI = 4)
- Nilai *Availability* yang diperoleh (NV = 3)

Maka Nilai Aset yang diperoleh yaitu:

Nilai Aset (SIM Akademik) = NC + NI + NV

= 3 + 4 + 3

= 10

Dari nilai yang didapatkan pada perhitungan Nilai Aset diatas dapat memberikan gambaran bahwa semakin besar nilai aset yang didapat maka semakin kritis pula nilai aset tersebut.

2.12.2 Identifikasi Ancaman (Threat) dan Kerentanan (Vulnerability)

Ancaman atau *Threat* adalah suatu potensi yang disebabkan oleh insiden yang tidak diinginkan yang mungkin membahayakan jalannya proses bisnis organisasi. Sedangkan kerentanan atau *Vulnerability* adalah kekurangan atau kelemahan di dalam prosedur keamanan informasi, perencanaan, implementasi atau kontrol internal di dalam organisasi terhadap penjagaan informasi yang dimiliki, dimana kelemahan ini dapat menimbulkan atau memicu ancaman (*threat*) (Sarno and Iffano, 2009).

Untuk melakukan identifikasi ancaman yang mungkin terjadi terhadap Informasi serta kerentanan yang dimiliki oleh Informasi sehingga dapat menimbulkan ancaman bagi Informasi tersebut, dapat dibuat tabel yang dinamakan tabel kemungkinan kejadian *(Probability of Occurrence).*

Dalam tabel kemungkinan kejadian gangguan keamanan tersebut, terdapat nilai rerata probabilitas seringnya kejadian terjadi, nilai tersebut dihasilkan dari klasifikasi probabilitas dengan rentang nilai yang dapat didefinisikan sebagai berikut:

- **LOW** : Nilai rerata probabilitas 0,1 – 0,3 (Jarang terjadi)
- **MEDIUM** : Nilai rerata probabilitas 0,4 – 0,6 (Beberapa kali terjadi)
- **HIGH** : Nilai rerata probabilitas 0,7 – 1,0 (Sering terjadi)

Berikut adalah contoh tabel kemungkinan kejadian gangguan keamanan informasi dilengkapi dengan nilai rerata probabilitasnya.

Tabel 2.6 Contoh kemungkinan kejadian gangguan keamanan informasi.

Kejadian	Jenis	Probabilitas	Rerata Probabilitas
Power Failure (Gangguan Sumber Daya)	*Vulnerable*	*Low*	0,1
Hardware Failure (Gangguan Perangkat Keras)		*Medium*	0,4
Fire (Kebakaran)	*Threat*	*Low*	0,1
Virus Attack (Serangan Virus)	*Threat*	*High*	0,7
Intruders (Penyusup: Hacker)	*Threat*	*Medium*	0,4
Data Corruption (Kerusakan Data)	*Vulnerable*	*Medium*	0,4
Data Missing Recipient (Kesalahan pengiriman data)	*Vulnerable*	*Low*	0,1
Nature Disaster (Bencana alam: Banjir, Gempa Bumi)	*Threat*	*Low*	0,2
Unauthorized Access (Akses Ilegal)	*Threat*	*Medium*	0,4

Sumber : (Sarno and Iffano, 2009)

Selanjutnya dengan berdasar tabel contoh diatas, dapat dihitung nilai ancaman (*Threat Value*) dari suatu aset. Perhitungan tersebut dapat dihitung menggunakan rumus berikut:

$$\textbf{\textit{Nilai Ancaman (NT)}} = \sum \textbf{\textit{PO}} \;/\; \sum \textbf{\textit{Ancaman}} \qquad (2.2)$$

Dimana:

$\sum$ ***PO*** **:** Jumlah rerata probabilitas

$\sum$ ***Ancaman*** **:** Jumlah ancaman terhadap informasi pada suatu aset

Contoh dari penerapan rumus perhitungan Nilai Ancaman suatu aset dapat dilihat pada tabel 2.xx dibawah ini;

Tabel 2.7 Contoh perhitungan Nilai Ancaman suatu aset.

Nama Aset: Mail Server			
Ancaman	**Jenis**	**Probabilitas**	**Rerata Probabilitas**
Power Failure (Gangguan Sumber Daya)	*Vulnerable*	*Low*	0,1
Hardware Failure (Gangguan Perangkat Keras)	*Vulnerable*	*Medium*	0,4
Virus Attack (Serangan Virus)	*Threat*	*High*	0,7

Intruders (Penyusup: Hacker)	*Threat*	*Medium*	0,4
Data Missing Recipient (Kesalahan pengiriman data)	*Vulnerable*	*Low*	0,1
Unauthorized Access (Akses Ilegal)	*Threat*	*Medium*	0,4
Jumlah Ancaman = 6	**Jumlah Rerara Probabilitas**		**2,1**

Sumber : (Sarno and Iffano, 2009)

Dari data tersebut dapat dihitung nilai ancaman (NT) dari Aset Mail server, yaitu:

$$NT \ (Mail\ Server) = \sum PO \ / \ \sum Ancaman$$
$$= 2{,}1 / 6$$
$$= 0{,}35$$

Dari hitungan Nilai Ancaman (NT) suatu aset, dapat dijelaskan bahwa semakin besat nilai NT maka semakin Kristis Aset tersebut.

2.12.3 Pengukuran Risiko

Setelah organisasi melakukan tahap identifikasi Aset serta penentuan nilai aset, yang dilanjutkan dengan melakukan analisis terhadap ancaman dan kerentanan informasi pada masing-masing aset, sehingga dapat memahami risiko yang akan dihadapi dan dampaknya terhadap organisasi jika terjadi kegagalan keamanan informasi. Maka tahap selanjutnya yang harus dilakukan yaitu melakukan pengukuran besaran Risiko dan evaluasi terhadap risiko, hal ini bertujuan agar organisasi memahami besaran risiko yang dihadapi pada setiap aset, dampak dari risiko yang dihadapi, apa penyebab utama dari risiko tersebut serta menentukan manajemen risiko yang berarti menerima risiko secara langsung, melakukan peredaman risiko dengan menggunakan kontrol yang tepat dan jika nilai risiko sangat tinggi serta tidak mungkin diatasi atau diredam oleh manajemen organisasi maka langkah yang harus dilakukan adalah mentransfer risiko tersebut kepada pihak lain.

a. Melakukan Analisis Dampak Bisnis (Business Impact Analysis)

Sebelum melangkah ke tahap pengukuran nilai risiko pada setiap aset informasi yang dimiliki, maka kita perlu melakukan pengukuran Analisis Dampak Bisnis atau yang biasa disebut dengan istilah BIA (*Business Impact Analysis*). BIA

adalah menggambarkan seberapa tahan proses bisnis di dalam organisasi berjalan jika informasi yang dimiliki terganggu. Analisis dampak bisnis dilakukan dengan menentukan skala nilai BIA, sebagaimana dicontohkan pada tabel 2.8 berikut:

Tabel 2.8 Contoh skala nilai BIA

Batas Toleransi Gangguan	***Keterangan***	***Nilai Skala***
< dari 1 minggu	*Not Critical*	0-20
1 hari s/d 2 hari	*Minor Critical*	21-40
< 1 hari	*Mayor Critical*	41-60
< 12 Jam	*High Critical*	61-80
< 1 Jam	*Very High Critical*	81-100

Sumber : (Sarno and Iffano, 2009)

Nilai yang tersebut pada tabel 2.8 diatas dapat diubah atau disesuaikan dengan kondisi pada organisasi. Setelah skala nilai BIA dapat didefinisikan selanjutnya dibuatlah tabel BIA untuk Aset Informasi yang dimiliki dengan mengacu pada nilai skala yang telah ditentukan pada tabel 2.8. Berikut adalah contoh tabel Nilai BIA untuk aset informasi yang dimiliki oleh organisasi.

Tabel 2.9 Contoh Nilai BIA Aset Informasi

Aset Informasi	***Impact (Dampak)***	***Nilai BIA***
Main Server	Operasi terhenti	95
Mail Server	Komunikasi dengan *User* tertunda	24
Database Server	Transaksi *on-line* terhenti	84
Web Server	Layanan *on-line* tertunda	15
LAN	Komunikasi antar bagian terhambat	25
Admin PC	Administrasi dan Pelaporan tertunda	22
Internet Connection	Komunikasi *on-line* terhenti	12

Sumber : (Sarno and Iffano, 2009)

b. Identifikasi Level Risiko

Setelah melakukan analisis probabilitas ancaman terhadap informasi dan menentukan nilai dampak terhadap bisnis organisasi (BIA), maka langkah selanjutnya adalah mengidentifikasi level risiko yang terjadi. Level risiko merupakan tingkat risiko yang timbul jika dihubungkan antara dampak bisnis (*impact*) dengan probabilitas ancaman yang mungkin terjadi.

Untuk mengidentifikasi risiko kita dapat membuat matriks level risiko dengan menggunakan nilai probabilitas ancaman dan nilai dampak (BIA). Misal nilai probabilitas ancaman dibagi menjadi 3 (tiga) level penilaian, yaitu:

0 < *Low Probability* < 0,1

0,1 < *Medium Probability* < 0,5

0,5 < *High Probability* < 1,0

Sedangkan nilai analisis dampak bisnis dibagi menjadi 5 (lima) level penilaian, yaitu:

0 < *Not Critical Impact* < 20

20 < *Low Critical Impact* < 40

40 < *Medium Critical Impact* < 60

60 < *High Critical Impact* < 80

80 < *Very High Critical Impact* < 100

Dari matriks level risiko ini memberikan identifikasi dan gambaran seberapa besar risiko yang diterima oleh organisasi jika terjadi kegagalan keamanan informasi. Dalam matriks tersebut dijelaskan bahwa level risiko yang mungkin diterima oleh organisasi dapat ditentukan berdasar hubungan probabilitas ancaman yang mungkin terjadi dengan dampak yang mungkin ditimbulkan. Berikut adalah contoh matriks level risiko:

Tabel 2.10 Matriks Level Risiko

Probabilitas Ancaman	**Dampak Bisnis (*Business Impact*)**				
	Not Critical (20)	***Low Critical (40)***	***Medium Critical (60)***	***High Critical (80)***	***Very High Critical (100)***
***Low* (0,1)**	Low 20 x 0,1 = 2	Low 40 x 0,1 = 4	Low 60 x 0,1 = 6	Low 80 x 0,1 = 8	Low 100 x 0,1 = 10
***Medium* (0,5)**	Low 20 x 0,5 = 10	Medium 40 x 0,5 = 20	Medium 60 x 0,5 = 30	Medium 80 x 0,5 = 40	Medium 100 x 0,5 = 50
***High* (1,0)**	Low 20 x 1,0 = 20	Medium 40 x 1,0 = 40	High 60 x 1,0 = 60	High 80 x 1,0 = 80	High 100 x 1,0 = 100

Sumber : (Sarno and Iffano, 2009)

c. Menghitung Nilai Risiko

Setelah penetapan matriks level risiko telah dilakukan, hal akhir yang harus dilakukan dalam menentukan risiko suatu aset informasi yaitu menghitung Nilai Risiko dari aset tersebut. Dalam menghitung Nilai Risiko ini menggunakan komponen nilai-nilai yang telah dihitung atau ditetapkan pada tahapan sebelumnya. Cara menilai risiko dapat dihitung dengan menggunakan persamaan matematika sebagai berikut:

Nilai Risiko (Risk Value) = NA x BIA x NT

Dimana:

- NA : Nilai Aset (*Asset Value*)
- BIA : Nilai Dampak Bisnis (*Business Impact Analysis*)
- NT : Nilai Ancaman (*Threat Value*)

Contoh menghitung risiko aset informasi dapat dilihat dengan penjelasan berikut:

Nama Aset: Mail server

Nila Aset (NA) = 5

Nilai BAI = 24

Nilai Ancaman (NT) = 0,35

Maka diperoleh Nilai Risiko untuk aset Mail Server, sebesar:

Nilai Risiko (Mail server) = NA x BIA x NT

= 5 x 24 x 0,35

= 42

Berdasar hitungan matematis yang digunakan untuk Aset Mail Server mendapat Nilai Risiko sebesar 42, selanjutnya kita lihat pada tabel matriks level risiko diatas dimana nilai tersebut masih dibawah 50, berarti Level Risiko untuk Aset Mail Server adalah MEDIUM.

2.12.4 Evaluasi dan Penanganan Risiko

Setelah organisasi melakukan analisis risiko dan mendapatkan nilai risiko dari masing-masing aset informasi yang dimiliki, selanjutnya organisasi harus

memahami risiko tersebut dan harus dapat membuat keputusan untuk menerima risiko tersebut secara langsung atau melakukan pengelolaan lebih lanjut terhadap manajemen yang ada sehingga aset yang memiliki nilai risiko tinggi masih dapat turunkan tingkat nilai risikonya sehingga risiko tersebut dapat diterima oleh organisasi.

Langkah yang harus dilakukan oleh organisasi selanjutnya dalam penanganan risiko keamanan informasi yaitu menentukan level penerimaan risiko. Level ini berfungsi sebagai kontrol organisasi untuk dapat menentukan sejauh mana suatu risiko keamanan informasi dapat diterima oleh organisasi atau bahkan risiko tersebut harus dilimpahkan ke pihak ketiga sebagai jaminan tetap berjalannya sistem dan menjaga keamanan informasi yang dimiliki. Adapun kriteria level penerimaan risiko dapat dikategorikan sebagai berikut:

1) Risiko Diterima (*risk acceptance*)
   Organisasi menerima risiko yang terjadi dengan segala dampaknya dan proses bisnis organisasi berlangsung terus.
2) Risiko direduksi (*risk reduction / mitigate*)
   Organisasi menerima risiko tetapi direduksi dengan menggunakan Kontrol keamanan sampai pada level yang dapat diterima oleh organisasi.
3) Risiko dihindari atau ditolak (*risk avoidance*)
   Organisasi menghindari risiko yang terjadi dengan cara menghilangkan penyebab timbulnya risiko atau organisasi menghentikan aktivitasnya jika gejala risiko muncul (seperti: mematikan server, memutus koneksi jaringan dan lain-lain).
4) Risiko dialihkan ke pihak ketiga (*risk transfer*)
   Organisasi menerima risiko yang ada dengan cara mengalihkan kepada pihak ketiga untuk mendapatkan penggantian atau kompensasi dari pihak ketiga tersebut (seperti: asuransi, vendor dan lain-lain).

Metode untuk menentukan kriteria penerimaan risiko dapat menggunakan tabel dengan matriks yang menghubungkan antar 3 (tiga) variabel yang ada, yaitu:

- Probabilitas ancaman (*threat probability*).
- Biaya pemulihan (*recovery cost*) akibat dampak dari penerimaan risiko.
- Biaya transfer risiko (*risk transfer cost*) kepada pihak ketiga.

Adapun matriks kriteria penerimaan risiko yang dapat dipakai oleh organisasi dapat dilihat pada tabel berikut:

Tabel 2.11 Matriks kriteria penerimaan risiko

Probabilitas Ancaman (PA)	**Biaya Pemulihan (BP)**		
	LOW	***MEDIUM***	***HIGH***
HIGH	*Risk Acceptance*	*Risk Avoidance*	*Risk Transfer*
MEDIUM	*Risk Acceptance*	*Risk Reduction*	*Risk Transfer*
LOW	*Risk Acceptance*	*Risk Reduction*	*Risk Transfer*
	HIGH	***MEDIUM***	***LOW***
	Biaya Transfer Risiko (BR)		

Sumber : (Sarno and Iffano, 2009)

Kriteria penerimaan risiko pada tabel diatas menggunakan prinsip logika AND, dapat dijelaskan sebagai berikut:

- Jika salah satu nilai variabel berlogika LOW, maka risiko diterima dan sebaliknya jika salah satu nilai variabel berlogika HIGH, maka risiko ditolak.
- Kriteria risiko diterima dapat dikembangkan dengan kriteria tambahan yaitu:
  a. Jika biaya pemulihan **Lebih Kecil** daripada biaya transfer risiko, maka risiko diterima dengan status *Risk Acceptance*.
  b. Jika biaya pemulihan **Lebih Besar** dari biaya transfer risiko, maka risiko diterima dengan status *Risk Transfer*.
  c. Jika biaya pemulihan **Sama Dengan** dari biaya transfer risiko, maka risiko diterima dengan status *Risk Reduction*, yaitu risiko direduksi dengan menggunakan pengendalian kontrol keamanan sampai pada level yang dapat diterima oleh organisasi, kecuali jika probabilitas ancaman bernilai **HIGH** maka risiko ditolak (*Risk Avoidance).*

BAB 3
METODOLOGI PENELITIAN

Pada bab ini akan diuraikan langkah-langkah penelitian dan penjelasan dari masing-masing langkah penelitian. Diagram alir tentang langkah penelitian atau metodologi penelitian ditunjukkan pada Gambar 3.1. Instrumen penelitian yang digunakan di antaranya adalah studi literatur atau pustaka, pengumpulan data, analisa hasil penelitian serta pengambilan kesimpulan dan saran.

Gambar 3.1 Gambaran Metodologi Penelitian

3.1 Studi Literatur

Studi literatur dalam penelitian ini digunakan untuk mendapatkan gambaran yang menyeluruh tentang apa yang sudah dikerjakan peneliti lain dan bagaimana peneliti mengerjakannya, kemudian mengidentifikasi celah penelitian sebagai dasar penelitian yang akan dilakukan. Penelitian dan kajian teori dari peneliti terdahulu dijadikan landasan berfikir untuk melakukan penelitian ini. Langkah-langkah dan teknis yang telah dijelaskan oleh penelitian yang terdahulu dikumpulkan dan dirangkum lalu diambil kesimpulan sehingga peneliti mendapatkan gambaran penyelesaian permasalahan terkait penyusunan kebijakan keamanan dan manajemen keamanan informasi.

Literatur yang digunakan sebagai acuan dalam penelitian ini merupakan hasil penelitian dari kalangan akademis yang disajikan dalam bentuk paper dalam jurnal, paper hasil seminar dan tesis.

Materi yang dikaji dalam literatur yang dibutuhkan pada penelitian ini yaitu tentang teori dan implementasi manajemen keamanan informasi serta kebijakan keamanan informasi.

3.2 Pengumpulan Data

Pengumpulan data pada penelitian ini dilakukan dengan beberapa tahap. Tahapan tersebut yaitu: (1) Identifikasi Aset; (2) Identifikasi Kerentanan dan Ancaman Keamanan; (3) Pengukuran Risiko; (4) Mitigasi Risiko. Adapun penjelasan dari setiap tahapan adalah sebagai berikut:

3.2.1 Identifikasi Aset

Proses ini dimulai dengan melakukan identifikasi semua proses bisnis pada organisasi. Selanjutnya dari proses bisnis dimulai identifikasi aset-aset yang dinilai penting dan kritikal. Identifikasi Aset ini meliputi identifikasi database organisasi, identifikasi software, identifikasi fisik, seperti server, router, dan informasi layanan jaringan. Identifikasi ini juga meliputi informasi apa yang melintasi jaringan, siapa, apa dan kapan data dapat diakses, dan juga jarak akses.

Selanjutnya dilakukan perangkingan tingkat kekritisan aset, khususnya yang menyangkut informasi utama yang menjadi nadi jalannya organisasi.

Tabel 3.1 Contoh tabel identifikasi Aset berdasar ISO 27001 Toolkit (ISO 27001, 2013)

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
1												
2												
3												
4												
5												
6												

3.2.2 Identifikasi Kerentanan dan Ancaman Keamanan

Ancaman atau *Threat* adalah suatu potensi yang disebabkan oleh insiden yang tidak diinginkan yang mungkin membahayakan jalannya proses bisnis organisasi. Sedangkan kerentanan atau *Vulnerability* adalah kekurangan atau kelemahan di dalam prosedur keamanan informasi, perencanaan, implementasi atau kontrol internal di dalam organisasi terhadap penjagaan informasi yang dimiliki, dimana kelemahan ini dapat menimbulkan atau memicu ancaman (*threat*) (Sarno and Iffano, 2009).

Penilaian kerentanan mempertimbangkan dampak potensial kerugian dari serangan yang sukses serta kerentanan fasilitas / lokasi terhadap serangan. Dampak kerugian adalah sejauh mana misi lembaga terganggu oleh serangan yang sukses dari ancaman yang diberikan. Komponen kunci dari penilaian kerentanan dengan benar mendefinisikan peringkat untuk dampak kerugian dan kerentanan.

Di dalam melakukan identifikasi kerentanan ini dilakukan dengan melakukan wawancara dan observasi langsung pada lokasi penelitian. Selanjutnya hasil dari identifikasi dilakukan verifikasi manual. Kerentanan tertentu dapat dinilai sesuai dengan tingkat risiko yang mereka ajukan kepada organisasi, baik secara internal maupun eksternal. Peringkat rendah dapat diterapkan untuk kerentanan yang rendah keparahan dan rendah dalam paparan. Kerentanan akan menerima peringkat tinggi jika tingkat keparahannya tinggi dan eksposurnya tinggi.

Dalam penelitan Rahmad, dkk, diidentifikasikan sebanyak lebih dari 70 (tujuh puluh) ancaman dan kerentanan yang dapat memberikan kerusakan dan

hilangnya keamanan pada aset informasi. Ancaman dan kerentanan tersebut dikelompokan menjadi 4 golongan besar, yaitu:

1. Alam
2. Lingkungan atau kesalahan teknis
3. Kesalahan Manasia (yang tidak disengaja)
4. Kesengajaan Manusia

Berikut adalah daftar ancaman dan kerentanan yang mengacu pada tabel Katalog threat berdasarkan Magerit dan ISO 27005 (Rahmad et al., 2010).

Tabel 3.2 Katalog ancaman (threat) pada aset informasi

Kode	Jenis Ancaman
***NARURAL* (ALAM)**	
N1	*Fire* (kebakaran)
N2	*Flood* (Banjir)
N3	*Lightning* (Petir)
N4	*Seismic phenomena* (gempa bumi)
N5	*Volcanic phenomena* (Gunung meletus)
N6	*Storm/hurricane* (Badai)
***Environmental or Technical Failure (*Lingkungan atau kesalahan teknis)**	
ET1	*Water damage* (Kebocoran)
ET2	*Electromagnetic interference from device* (Pengaruh gelombang elektromaknetik perangkat)
ET3	*Industrial electromagnetic explosion* (Ledakan gelombang elektromagnetik)
ET4	*Short Circuit* (Konsleting*)*
ET5	*Power failure* (Kerusakan sumber listrik*)*
ET6	*Pollution* (Polusi*)*
ET7	*Hardware failure* (kerusakan perangkat keras*)*
ET8	*Network failure* (kerusakan jaringan komputer*)*
ET9	*Software failure* (kerusakan perangkat lunak)
ET10	*Unsuitable temperature or/and humidity conditions* (Kelainan temperatur udara)
ET11	*Media degradation* (Degradasi Media)
ET12	*HVAC failure* (Kerusakan HVAC)
***Human Accidental (*Kesalahan Manasia (yang tidak disengaja))**	
HA1	*User's error* (Kesalahan user)
HA2	*Administrator's error* (Kesalahan administrator)
HA3	*Configuration Error* (Kesalahan konfigurasi)
HA4	*Organizational deficiencies* (kekurangan (cacat) organisasi)
HA5	*Malware diffusion* (pembauran Malware)
HA6	*[Re]-routing error* (kesalahan routing data)
HA7	*Sequence error* (kesalahan urutan)
HA8	*Information leaks* (kebocoran informasi)
HA9	*Information modification* (modifikasi informasi)
HA10	*Incorrect information entry* (salah memasukkan informasi)

Kode	Jenis Ancaman
HA11	*Information degradation* (Degradasi informasi)
HA12	*Configuration Error* (Kesalahan konfigurasi)
HA13	*Disclosure of information* (Keterbukaan informasi)
HA14	*Bug on software* (bug (kesalahan) software)
HA15	*Defects in software maintenance or updating* (Cacat dalam pemeliharaan atau pembaruan perangkat lunak)
HA16	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)
HA17	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)
HA18	*System failure due to exhaustion of resources* (Kegagalan sistem karena kehabisan sumber daya)
HA19	*Staff shortage* (Kekurangan staf)
Human Deliberate **(Kesengajaan Manusia)**	
HD1	*Spying by a foreign state or a mafia (using important resources)* (Memata-matai oleh negara asing atau mafia)
HD2	*Vandalism from outside: bullets or objects thrown from the street, etc.* (Vandalisme dari luar: peluru atau benda yang dilemparkan dari jalan, dll.)
HD3	*Vandalism from inside: by people authorized within the premises (personnel, sub-contractor, etc.).* (Vandalisme dari dalam: oleh orang-orang yang diberi wewenang di dalam bangunan (personel, sub-kontraktor, dll.).
HD4	*Terrorism: sabotage, explosives left close to sensitive premises* (Terorisme: sabotase, bahan peledak dekat dengan tempat sensitif)
HD5	*Hardware theft* (Pencurian perangkat keras)
HD6	*Network equipment theft* (Pencurian perangkat jaringan)
HD7	*Malicious erasure of networking configurations* (Penghapusan berbahaya konfigurasi jaringan)
HD8	*Malicious erasure of hardware configurations* (Penghapusan berbahaya konfigurasi perangkat keras)
HD9	*Saturation of the network caused by a worm* (Kejenuhan jaringan disebabkan oleh worm)
HD10	*Malicious and repeated saturation of IT resources by a group of users* (Sumber daya TI berbahaya dan berulang oleh sekelompok pengguna)
HD11	*Distorted data entry or fiddling of data* (Entri data terdistorsi atau mengutak-atik data)
HD12	*Intentional erasure (direct or indirect), theft or destruction of program or data containers* (Penghapusan yang disengaja (langsung atau tidak langsung), pencurian atau penghancuran wadah program atau data)
HD13	*Intended access to data or information and disclosure of information* (Dimaksudkan akses ke data atau informasi dan pengungkapan informasi)
HD14	*Document or media theft* (Pencurian dokumen atau media)
HD15	*Malicious erasure (directly or indirectly) of software on its storage* (Penghapusan berbahaya (langsung atau tidak langsung) dari perangkat lunak pada penyimpanannya)

Kode	Jenis Ancaman
HD16	*Malicious modification (direct or indirect) of the functionalities of a program or of the operation of an office program (Excel, Access, etc)* Modifikasi berbahaya (langsung atau tidak langsung) dari fungsionalitas suatu program atau pengoperasian program perkantoran (Excel, Access, dll)
HD17	*Illegal usage of software* (Penggunaan perangkat lunak secara ilegal)
HD18	*Intrusion to system by third party whose contract with organization* (Intrusion ke sistem oleh pihak ketiga yang kontraknya dengan organisasi)
HD19	*Malicious erasure of software configurations* (Penghapusan berbahaya konfigurasi perangkat lunak)
HD20	*Absence or strike of IT operational personnel* (Tidak ada atau mogok personil operasional TI)
HD21	*Masquerading of user identity* (Penyamaran identitas pengguna)
HD22	*Abuse of access privileges* (Penyalahgunaan hak akses)
HD23	*Software misuse* (Penyalahgunaan perangkat lunak)
HD24	*Hardware misuse* (Penyalahgunaan perangkat keras)
HD25	*Network misuse* (Penyalahgunaan jaringan)
HD26	*Document misuse* (Penyalahgunaan dokumen)
HD27	*Unauthorized access* (Akses yang tidak sah)
HD28	*Traffic analysis* (Analisis lalu lintas)
HD29	*Eavesdropping* (Menguping)
HD30	*Software manipulation* (Manipulasi perangkat lunak)
HD31	*Denial of service* (Kegagalan layanan)
HD32	*Extortion* (Pemerasan)
HD33	*Social engineering*

Sumber: Rahmad et al., 2010, diolah

3.2.3 Pengukuran Risiko

Setelah identifikasi kerentanan dan ancaman telah dilakukan dan didapatkan semua elemen yang dapat mempengaruhi keamanan informasi beserta infrastrukturnya. Maka selanjutnya dilakukan pengukuran tingkat besaran risiko, dengan melakukan pemetaan pada tabel.

Analisis pengukuran ini melibatkan opsi kontrol untuk setiap ancaman dengan mempertimbangkan biaya, pengurangan risiko, kemungkinan terjadinya ancaman, dan nilai aset.

Berikut adalah contoh tabel pengukuran risiko, yang diambil dari iso/iec 27001 toolkit.

Tabel 3.3 Tabel pengukuran risiko

No	Nama Aset	Merek / Type	Nilai NA	Nilai BIA	Nilai NT	Nilai Risiko	Level Risiko
1							
2							
3							
4							
5							
6							
7							

Nilai Risiko didapat dengan melakukan perkalian antara Nilai Aset (NA), Nilai analisis dampak bisnis (BIA) dan Nilai Ancaman (NT), yang mana cara penghitungan nilai-nilai tersebut telah dijelaskan pada bab 2.

3.2.4 Mitigasi Risiko dan Kontrol

Mitigasi Risiko adalah suatu tindakan terencana dan berkelanjutan yang dilakukan oleh pemilik risiko agar bisa mengurangi dampak dari suatu kejadian yang berpotensi atau telah merugikan atau membahayakan pemilik risiko tersebut. Mitigasi risiko identik dengan memindahkan risiko yang akan dihadapi untuk ditanggung oleh pihak luar atau asuransi. Dalam melalukan tahapan analisa mitigasi yang harus diperhatikan adalah tingkat kematangan risiko yang dihadapi dan juga anggaran yang harus dikeluarkan.

3.3 Analisis Hasil dan Penyusunan Draf Kebijakan

Setelah tahapan pemetaan kontrol ISO 27001 selesai dilakukan maka dengan mempertimbangkan hasil analisis tersebut langkah selanjutnya adalah melakukan penyusunan draf kebijakan keamanan informasi. Dalam penyusunan draf kebijakan keamanan informasi ini harus memenuhi beberapa elemen dan atribut penting yang ada pada sebuah dokumen kebijakan keamanan.

Adapan penjelasan dari elemen yang harus melekat pada sebuah dokumen kebijakan keamanan informasi adalah:

a. Tujuan Kebijakan

   Berisikan gambaran umum dari tujuan pembuatan dokumen kebijakan keamanan informasi.

b. Ruang lingkup

   Memberikan gambaran yang jelas terhadap ruang lingkup dan batasan dari kebijakan yang dibuat. Di dalam ruang lingkup ini juga dapat dijelaskan sarana dan prasarana serta proses yang tercakup di dalam.

c. Tanggung Jawab dan peran

   Berisikan kejelasan peran dan tanggung jawab masing-masing personal organisasi di dalam mengelola keamanan informasi. Termasuk kontak personal yang harus dihubungi bila suatu ancaman terjadi.

d. Tujuan Keamanan Informasi

   Berisikan tujuan menyeluruh dari pelaksanaan manajemen keamanan informasi yang mencakup pemenuhan 3 (tiga) aspek CAI, yaitu kerahasiaan, keutuhan dan ketersediaan.

e. Penilaian Kerentanan dan Ancaman

   Memberikan gambaran singkat tentang hasil analisa penilaian ancaman dan kerentanan risiko keamanan informasi, khususnya pada aspek yang memilki risiko tinggi.

f. Dokumen penunjang

   Berisikan daftar dokumen penunjang dalam implementasi kebijakan keamanan tersebut. Dokumen ini bisa berupa undang-undang pemerintah, kebijakan organisasi, prosedur dan petunjuk penggunaan.

3.4 Verifikasi dan Validasi

Verifikasi dilakukan dengan tujuan memastikan kebenaran dari informasi yang termuat dalam dokumen kebijakan keamanan informasi dan kesesuaiannya dengan kondisi DPTSI ITS. Metode yang digunakan dalam melakukan verifikasi adalah melakukan wawancara dengan bagian DPTSI ITS sebagai pihak yang memiliki kewenangan dalam keamanan teknologi informasi.

Validasi dilakukan untuk memastikan dokumen kebijakan keamanan informasi dapat berjalan sesuai dengan kondisi yang ada pada DPTSI ITS dan untuk

menemukan ketidaksesuaian dan kekurangan kebijakan keamanan informasi sehingga dapat dibenahi sesuai kondisi yang ada. Metode yang digunakan adalah dengan pengujian kebijakan keamanan informasi dengan pelaksana kebijakan keamanan informasi yaitu pihak manajemen DPTSI ITS.

3.5 Penyusunan Kesimpulan

Penarikan kesimpulan dilakukan dengan mengacu dari hasil uji coba yang telah dilakukan dan juga hasil Analisa data yang dilakukan. Selanjutnya dilakukan penulisan saran akan tindak lanjut penelitian yang selanjutnya.

[Halaman ini sengaja dikosongkan]

BAB 4
HASIL DAN PEMBAHASAN

Pada bab ini menjelaskan masing-masing proses dan hasil yang didapatkan dari setiap tahap penelitian yang dilakukan sebagaimana dijelaskan pada bab 3. Diawali dengan tahap identifikasi aset yang terkait sistem informasi, dilanjutkan dengan identifikasi risiko sampai dengan mitigasi risiko yang harus dilakukan. Selanjutnya hasil dari pemetaan risiko aset tersebut akan dijadikan landasan dalam pembuatan kebijakan keamanan informasi organisasi.

4.1 Proses Identifikasi Aset

Setelah melakukan studi literasi, langkah selanjutnya yang dilakukan pada penelitian ini yaitu pengumpulan data. Data yang dimaksud yaitu data aset yang dimiliki oleh kampus ITS khususnya DPTSI yang bertanggungjawab dengan proses lalu lintas informasi yang terjadi pada keseharian kehidupan kampus. Proses identifikasi aset ini dilakukan dengan cara wawancara, observasi langsung dan olah database.

Sebelum melangkah lebih lanjut, perlu diperjelas definisi Aset informasi, khususnya dalam ruang lingkup keamanan informasi. Yang dimaksud dengan aset infromasi yaitu segala item atau perangkat yang dapat mendukung kegiatan terkait informasi, yang terdiri dari perangkat keras, perangkat lunak, data, dan informasi; orang yang mendukung dan menggunakan sistem TI; peralatan komunikasi; dan berbagai sistem layanan (Deloitte Australia et al., 2016). Sedangkan ISO/IEC 27000:2009 menyebutkan bahwa aset informasi adalah segala sesuatu yang dapat memberikan nilai pada organisasi, termasuk didalamnya yaitu informasi, perangkat lunak (program komputer), perangkat fisik (komputer), layanan, manusia dan aset tak berwujud, seperti reputasi dan *image.*

Pada bab ini aset akan dikelompokkan menjadi 2 (dua) yaitu: aset utama dan aset pendukung.

1. Aset utama adalah aset yang merupakan aset sistem dan database. Aset informasi tersebut meliputi data mahasiswa, data akademik, data kepegawaian dan

kepangkatan, data keuangan, data perencanaan, data penelitian dan paten, data email dan SSO (*single sign on*) serta data *warehouse* yang menjadi pangkalan pengolahan laporan perkembangan organisasi dimana data-data tersebut melekat dengan aplikasi SIM (*system information management*) yang tersedia.

Berdasar laporan borang akreditasi perguruan tinggi ITS, saat ini terdapat sedikitnya 35 sistem informasi yang berjalan di ITS untuk mendukung proses bisnis organisasi ITS.

2. Aset pendukung adalah aset yang berupa aset perangkat keras (*hardware),* jaringan komputer *(network),* perangkat lunak (software) dan media penyimpanan (Storage). Baik itu perangkat yang berhubungan langsung dengan layanan lalu lintas informasi maupun hanya sebagai pendukung berjalannya layanan lalu lintas informasi, seperti perangkat pendingin ruangan (AC), genset, UPS, CCTV dan yang sebagainya.

Kampus ITS sebagai bagian dari Kementerian Pendidikan dan Kebudayaan Republik Indonesia, tentunya melakukan pengelolaan aset sebagaimana yang telah ditetapkan oleh Pemerintah Indonesia karena aset yang dikelola adalah termasuk Barang Milik Negara (BMN).

Berdasar rekapitulasi laporan sistem informasi e-Aset, DPTSI memiliki 1.212 aset BMN yang dikelola, baik aset yang terkait layanan informasi maupun aset pendukung perkantoran. Dari 1.212 aset yang tercatat tersebut tidak semua dalam kondisi baik dan dapat digunakan. Terdapat lebih kurang 20% aset yang dalam kondisi rusak berat dan menunggu proses penghapusan.

Untuk menentukan tingkat kerusakan aset BMN tersebut, telah diatur oleh pemerintah Indonesia melalui PP No. 6 tahun 2006 tentang Pengelolaan Barang Milik Negara/Daerah yang disempurnakan dengan PP No. 27 tahun 2014 tentang Pengelolaan Barang Milik Negara/Daerah dan diperjelas dengan Peraturan Menteri Keuangan RI No. 181/PMK.06/2016 tentang Penatausahaan Barang Milik Negara, dijelaskan pada Lampiran II, bahwa kondisi BMN dibedakan menjadi 3 (tiga) kriteria, yakni Baik (B) , Rusak Ringan (RR) , dan Rusak Berat (RB). Dan pada Lampiran V, dijelaskan dari masing-masing kriteria tersebut, yaitu:

- Peralatan dan Mesin, dan Aset Tetap Lainnya
  a. Baik (B), Apabila kondisi barang tersebut masih dalam keadaan utuh dan berfungsi dengan baik.
  b. Rusak Ringan (RR), Apabila barang tersebut masih dalam keadaan utuh, tetapi kurang berfungsi dengan baik. Untuk berfungsi dengan baik memerlukan perbaikan ringan dan tidak memerlukan penggantian bagian utama/ komponen pokok.
  c. Rusak Berat (RB), Apabila kondisi barang tersebut tidak utuh dan tidak berfungsi lagi atau memerlukan perbaikan besar/ penggantian bagian utama/ komponen pokok, sehingga tidak ekonomis lagi untuk diadakan perbaikan/ rehabilitasi (Kementerian Keuangan, 2016).

  Sedangkan informasi tentang masa manfaat (umur) suatu aset BMN, ditetapkan oleh pemerintah Indonesia dengan mengeluarkan Keputusan Menteri Keuangan No. 59/KMK.6/2013 Tentang Tabel Masa Manfaat Dalam Rangka Penyusutan Barang Milik Negara Berupa Aset Tetap Pada Entitas Pemerintah Pusat, dimana disebutkan di dalamnya bahwa masa manfaat dari peralatan komputer dan sejenisnya adalah 4 tahun (Kementerian Keuangan, 2013).

Adapun rincian dari jumlah aset kondisi baik dan rusak berat dapat dilihat pada tabel 4.1 dibawah ini.

Tabel 4.1 Jumlah Aset yang dikelola oleh DPTSI

Kategori Aset	Jumlah	Kondisi Baik	Kondisi Rusak Berat
Aset Informasi dan Pendukungnya	670	506	164
Aset Perkantoran (Non TI)	542	479	63
Total	**1212**	**985**	**227**

Sumber: diolah, 2019

Dalam melakukan penelitian ini aset yang akan diolah datanya adalah aset informasi dan pendukungnya saja. Selanjutnya aset-aset tersebut dipilah dan dikelompokkan berdasarkan fungsi dan kategori aset.

Berikut adalah 4.1. yang berisikan daftar pengelompokan aset yang dikelola oleh DPTSI ITS per juni 2019.

Tabel 4.2 Pengelompokan Aset

No	Nama Aset	Jenis Aset
1	SI Akademik	Data / *Information System*
2	SI Pendaftaran Seleksi Masuk ITS (SIMITS)	
3	SI Pendataan Mahasiswa Baru ITS (SIPMABA)	
4	SIM Kemahasiswaan (SKEM)	
5	SI Satuan Angka Kredit (SAR Online)	
6	SI Yudisium	
7	SI Kurikulum	
8	SI Penjadwalan Ruang (SIMARU)	
9	SI Beasiswa	
10	SI Perencanaan, Monitoring dan Evaluasi (SIPMONEV)	
11	SIM Rencana Belanja Anggaran (SIM RBA)	
12	SIM Keuangan	
13	SI Monitoring Pendapatan ITS (SIMONDITS)	
14	SI Asrama	
15	Host-to-host App	
16	e-Perkantoran	
17	SIM Kepegawaian	
18	SIM Entry SK	
19	SIM Penilaian Kinerja Tendik dan Dosen	
20	SIM Insentif Kinerja (IKITS)	
21	Sistem ODOO ERP	
22	SIM Persediaan	
23	SIM Inventori (E-Aset)	
24	Ad Hoc Reporting	
25	Sistem Informasi Pelaporan Data	
26	Executive Reporting	
27	SIM Penelitian ITS (SIMPel)	
28	SI Resource ITS (RESITS)	
29	ITS Alumni Data Tracking System	
30	Service Desk ITS (E-ticket)	
31	SIM Kepangkatan (SIKEPANG)	
32	SIM Beban Kerja Dosen (BKD)	
33	Single Sign On (SSO) App	
34	SIM Kearsipan	
35	PDDIKTI Integrator	
36	ITS Website	
37	Academic VMware vSphere 6	

No	Nama Aset	Jenis Aset
38	Microsoft SQL Server Enterprise	Perangkat Lunak dan Lisensi
39	Microsoft SQL Server Standart	
40	Microsoft Windows Server Standart	
41	Microsoft Windows Server DataControl	
42	Visual Studio Profesional	
43	Visio Profesional	
44	Microsoft Windows Entreprise	
45	Microsoft Office Pro Plus	
46	Software Decision Support System (DSS)	
47	Adobe Creative Suite 5 Master	
48	ApexSQL Universal Studio	
49	Microsoft Windows Server Enterprise	
50	PHP Maker v2018.0.8	
51	Fortinet	
52	iThenticate	
53	Certificate SSL Verisign	
54	Jaringan Fiber Optic (BackBone)	Perangkat Jaringan
55	Server Database	
56	Server VM / Applications	
57	Server Development	
58	Server SSO	
59	Switch Datacenter	
60	Switch Core	
61	Switch Distribution	
62	Switch Access	
63	Switch SAN	
64	Modulas Monitoring System	
65	Router	
66	Firewall	
67	Load Balancer	
68	Wireless Access Point	
69	Rak Server	
70	Rackmount	
71	Printer	Perangkat Keras
72	Scanner	
73	CCTV - Camera Control Television System	
74	Alat Sidik Jari	
75	Uninterruptible Power Supply (UPS)	
76	Camera Conference	

No	Nama Aset	Jenis Aset
77	Telephone (PABX)	
78	Pesawat Telephone	
79	Telephone Mobile	
80	Genset	
81	Personal Computer (PC Unit)	
82	Notebook	
83	Mobile PC (Tablet)	
84	KVM (Keyboard Video Monitor)	
85	SAN Storage	Media penyimpanan
86	Portable Harddisk	

Sumber : SIM Inventori DPTSI dan wawancara

Setelah pemilahan aset dilakukan langkah selanjutnya yaitu melakukan penghitungan nilai aset pada tiap-tiap aset yang ada sesuai dengan aspek keamanan informasi yaitu Nilai kerahasiaan (c*onfidentiality value*), Nilai integritas (*integrity value*) dan Nilai ketersediaan (*availability value*) yang merupakan aspek dasar untuk mengidentifikasi aset kritis. Proses penghitungan nilai aset tersebut menggunakan acuan tabel yang telah dijelaskan pada Bab 2. Adapun rumus yang digunakan untuk menghitung nilai aset adalah sebagaimana berikut:

$$\textit{Nilai Aset (NA)} = NC + NI + NV$$

Dimana:

NA = Nilai Aset yang didapatkan

NC = Nilai *Confidentiality* sesuai dengan nilai yang ada di tabel

NI = Nilai *Integrity* sesuai dengan nilai yang ada di tabel

NV = Nilai *Availability* sesuai dengan nilai yang ada di tabel

Hasil dari penghitungan Nilai Aset pada semua aset informasi yang dikelola oleh DPTSI ITS, dapat dilihat pada lampiran 2. Selanjutnya dilakukan proses filter nilai aset yang dinyatakan sebagai aset kritis. Berdasarkan tabel yang dibuat, maka ditentukan bahwa aset dianggap kritis jika nilai aset lebih besar dari 6.

Setelah dilakukan penghitungan nilai aset, didapatkan **205** aset yang memiliki nilai aset lebih dari 6. Selanjutnya dilakukan pengelompokan aset berdasarkan jenis aset, merek, tahun perolehan dan fungsi aset.

Adapun hasil penilaian aset kritis terhadap aspek keamanan informasi CIA, dapat dilihat pada tabel 4.2 sebagai berikut:

Tabel 4.3 Hasil penghitungan Nilai Aset (Asset Value) kritis berdasar aspek keamanan informasi CIA

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	Merek / Type	Jumlah Aset	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Nilai Aset
1	DPTSI	BAPKM	SI Akademik		1			Information System	3	4	3	10
2	DPTSI	Biro Keuangan	SIM Rencana Belanja Anggaran (SIM RBA)		1			Information System	2	3	2	7
3	DPTSI	Biro Keuangan	SIM Keuangan		1			Information System	2	3	4	9
4	DPTSI	DIRPAL	SI Monitoring Pendapatan ITS (SIMONDITS)		1			Information System	2	3	4	9
5	DPTSI	Biro Keuangan	Host-to-host App		1			Information System	2	3	4	9
6	DPTSI	Biro Umum	SIM Kepegawaian		1			Information System	2	3	3	8
7	DPTSI	DPTSI	Sistem Informasi Pelaporan Data		1			Information System	2	2	3	7
8	DPTSI	DPTSI	Executive Reporting		1			Information System	2	2	3	7
9	DPTSI	DPTSI	Single Sign On (SSO) App		1			Information System	4	4	4	12
10	DPTSI	DPTSI	Modulas Monitoring System	Modul	1	2009	Network Backbone	Network Device	2	2	3	7
11	DPTSI	DPTSI	Fiber Optic Operating	GE	1	2010	Network Backbone	Network Device	3	4	4	11
12	DPTSI	DPTSI	Interface Network	CISCO	1	2010	Network Backbone	Network Device	3	3	4	10
13	DPTSI	DPTSI	Paralel Control Network	CISCO	1	2010	Network Backbone	Network Device	3	3	4	10
14	DPTSI	DPTSI	Internet Network	CISCO	1	2010	Network Backbone	Network Device	3	3	4	10

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	Merek / Type	Jumlah Aset	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Nilai Aset
15	DPTSI	DPTSI	Server	HPE DL580 Gen9 CTO SVR	2	2017	OLTP server dan OLAP Server	Network Device	3	4	4	11
16	DPTSI	DPTSI	Server	HPE DL380 Gen9 CTO Derver	4	2017	VMWare 65 Server	Network Device	3	4	4	11
17	DPTSI	DPTSI	Server	HPE MSA 2040 SAN	1	2017	Database Storage	Network Device	3	4	4	11
18	DPTSI	DPTSI	Server	HP / PROLIANT ML150	3	2005	Server Aplikasi Unit	Network Device	3	4	4	11
19	DPTSI	DPTSI	Server	Advance Server SUN X4100	2	2009	Data Center	Network Device	3	4	4	11
20	DPTSI	DPTSI	Server	HP PROLIANT DL380G6	1	2010	Server Aplikasi Unit	Network Device	3	4	4	11
21	DPTSI	DPTSI	Server	HPPROLIANT DL 145 R G3,AMD OPTERON2.2 GHZ.MON 15	4	2010	Server Aplikasi Unit	Network Device	3	4	4	11
22	DPTSI	DPTSI	Server	UPS ICA RN 3200C	3	2011	UPS Server	Network Device	3	4	4	11
23	DPTSI	DPTSI	Server	HP DL580R07 CTO Chassis (Database)	1	2011	Database Server	Network Device	3	4	4	11
24	DPTSI	DPTSI	Server	HP DL380E	4	2012	HyperV Server	Network Device	3	4	4	11
25	DPTSI	DPTSI	Server	HP/Proliant DL380G7	2	2012	Proxmox VE Server	Network Device	3	4	4	11
26	DPTSI	DPTSI	Server	HP/DL580	2	2014	VMWare 22 Server	Network Device	3	4	4	11
27	DPTSI	DPTSI	Server	DELL/PowerEdge R230	1	2016	Hosting zeus Server	Network Device	3	4	4	11
28	DPTSI	DPTSI	Server	HPE/Proliant DL580 Gen10	1	2018	Proxmox VE Server	Network Device	3	4	4	11

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	Merek / Type	Jumlah Aset	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Nilai Aset
29	DPTSI	DPTSI	Server	HPE/ProLiant DL380 Gen10	5	2018	Proxmox VE Server	Network Device	3	4	4	11
30	DPTSI	DPTSI	Wireless Access Point	Cisco/AIR-CAP2702I-F	5	2016	Distributor Wireless AP	Network Device	1	3	4	8
31	DPTSI	DPTSI	Wireless Access Point	CISCO Aironet 1852E	3	2017	Distributor Wireless AP	Network Device	1	3	4	8
32	DPTSI	DPTSI	Wireless Access Point	CISCO Aironet 3802E	3	2017	Distributor Wireless AP	Network Device	1	3	4	8
33	DPTSI	DPTSI	Firewall	Barracuda 641 ADC	4	2017	Network Firewall	Network Device	2	4	4	10
34	DPTSI	DPTSI	Firewall	Firewall Cisco ASA 5585-X	1	2011	Network Firewall	Network Device	2	4	4	10
35	DPTSI	DPTSI	Router	Gigabit Router Cisco 3945	1	2011	Main Router	Network Device	2	4	3	9
36	DPTSI	DPTSI	Router	CISCO 7606 S	1	2012	Core Router	Network Device	2	4	3	9
37	DPTSI	DPTSI	Router	Cisco ASR 1002X	1	2016	Core BGP router	Network Device	2	4	4	10
38	DPTSI	DPTSI	Router	RB 1100 HX2	4	2013	Internet Access	Network Device	2	4	4	10
39	DPTSI	DPTSI	Auto Switch/Data Switch	CISCO 4900	9	2010	Access Switch	Network Device	2	4	3	9
40	DPTSI	DPTSI	Auto Switch/Data Switch	CISCO 3560	45	2010	Access Switch	Network Device	2	4	3	9
41	DPTSI	DPTSI	Auto Switch/Data Switch	HPE 1820	11	2018	Access Switch	Network Device	2	4	3	9
42	DPTSI	DPTSI	Auto Switch/Data Switch	CISCO 3560	1	2018	Access Switch	Network Device	2	4	3	9
43	DPTSI	DPTSI	Switch	Nexus N9K-C93120TX bundle 2pcs	1	2017	Database Data Switch	Network Device	2	4	4	10

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	Merek / Type	Jumlah Aset	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Nilai Aset
44	DPTSI	DPTSI	Switch	Cisco Catalyst 3560X 24 Port	1	2011	Access Switch	Network Device	2	4	3	9
45	DPTSI	DPTSI	Switch	TP-Link	3	2013	Access Switch	Network Device	2	4	3	9
46	DPTSI	DPTSI	Switch	Cisco/WS-C4900M	1	2014	Distributor Switch	Network Device	2	4	4	10
47	DPTSI	DPTSI	Switch	HP 1820	2	2016	Access Switch	Network Device	2	4	3	9
48	DPTSI	DPTSI	Switch	HPE/FlexFabric 5940	1	2018	Datacentre Access Switch	Network Device	2	4	4	10
49	DPTSI	DPTSI	Switch	Huawei 12700	1	2016	Core Switch	Network Device	2	4	4	10
50	DPTSI	DPTSI	Switch	Cisco 6500	1	2016	Core Switch	Network Device	2	4	4	10
51	DPTSI	DPTSI	Switch	Cisco 7700	1	2016	Core Switch	Network Device	2	4	4	10
52	DPTSI	DPTSI	Storage Modul Disk (Peralatan Mainframe)	SAN/Storage	2	2012	Data Centre	Storage Device	3	4	4	11
53	DPTSI	DPTSI	Storage Modul Disk (Peralatan Mainframe)	Hitachi/HUS110	1	2014	Data Centre	Storage Device	3	4	4	11
54	DPTSI	DPTSI	Stabilizer/UPS	UPS Protekta	1	2009	UPS Server	Hardware	1	2	4	7
55	DPTSI	DPTSI	Uninterupted Power Supply (UPS)	Rackmounted TCL3300	1	2012	UPS Server	Hardware	1	2	4	7
56	DPTSI	DPTSI	Genset	CATERPILLAR ECW00427	1	2015		Hardware	1	2	4	7
57	DPTSI	DPTSI	A.C. Split	Type CS-D43DB4H5 (5 HP)	1	2010	Data Center AC	Hardware	2	3	4	9
58	DPTSI	DPTSI	A.C. Split	Panasonic	3	2013	Data Center AC	Hardware	2	3	4	9

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	Merek / Type	Jumlah Aset	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Nilai Aset
59	DPTSI	DPTSI	A.C. Split	Daikin STNE	4	2016	Data Center AC	Hardware	2	3	4	9
60	DPTSI	DPTSI	CCTV - Camera Control Television System	Hikvision	38	2018	Kamera Pengaman	Hardware	1	3	4	8
61	DPTSI	DPTSI	Alat Sidik Jari	FInger Prnt	1	2014	Pengaman Pintu	Hardware	3	4	4	11

Sumber: Diolah, 2019

4.2 Identifikasi Ancaman (Threat) dan Kerentanan (Vulnerability)

Pada tahap ini diawali dengan melakukan pendataan ancaman dan kerentanan yang sering terjadi pada aset teknologi informasi. Adapun pada penelitian ini daftar ancaman dan kerentanan keamanan informasi mengacu pada tabel Katalog threat berdasarkan Magerit dan ISO 27005 (Rahmad et al., 2010).

Dari tabel katalog tersebut dilakukan penilaian probabilitas kemungkinan ancaman dan kerentanan terjadi pada DPTSI ITS. Penilaian tersebut mengacu pada penjelasan pada Bab 2 sub bab 2.12.2.

Pada tabel daftar ancaman dan kerentanan diberikan penilaian terhadap kemungkinan (probabilitas) terjadinya ancaman tersebut terhadap aset informasi. Adapun tabel ancaman dan kerentanan terlihat dapat dilihat pada tabel 4.4 berikut.

Tabel 4.4 Katalog ancaman (threat) pada aset informasi beserta nilai probabilitas

Kode	Jenis Ancaman	Probabilitas	Rerata Probabilitas
N1	*Fire* (kebakaran)	Low	0,1
N2	*Flood* (Banjir)	Low	0,1
N3	*Lightning* (Petir)	Low	0,1
N4	*Seismic phenomena* (gempa bumi)	Low	0,1
N5	*Volcanic phenomena* (Gunung meletus)	Low	0,1
N6	*Storm/hurricane* (Badai)	Low	0,1
ET1	*Water damage* (Kebocoran)	Low	0,1
ET2	*Electromagnetic interference from device* (Pengaruh gelombang elektromaknetik perangkat)	Low	0,3
ET3	*Industrial electromagnetic explosion* (Ledakan gelombang elektromagnetik)	Low	0,1
ET4	*Short Circuit* (Konsleting)	Medium	0,4
ET5	*Power failure* (Kerusakan sumber listrik)	Low	0,1
ET6	*Pollution* (Polusi)	Low	0,1
ET7	*Hardware failure* (kerusakan perangkat keras)	Medium	0,4
ET8	*Network failure* (kerusakan jaringan komputer)	Medium	0,4
ET9	*Software failure* (kerusakan perangkat lunak)	Low	0,3

Kode	Jenis Ancaman	Probabilitas	Rerata Probabilitas
ET10	*Unsuitable temperature or/and humidity conditions* (Kelainan temperatur udara)	Low	0,1
ET11	*Media degradation* (Degradasi Media)	High	0,8
ET12	*HVAC failure* (Kerusakan HVAC)	Low	0,1
HA1	*User's error* (Kesalahan user)	Medium	0,4
HA2	*Administrator's error* (Kesalahan administrator)	Medium	0,4
HA3	*Configuration Error* (Kesalahan konfigurasi)	Low	0,3
HA4	*Organizational deficiencies* (kekurangan (cacat) organisasi)	Low	0,1
HA5	*Malware diffusion* (pembauran Malware)	Medium	0,4
HA6	*[Re]-routing error* (kesalahan routing data)	Low	0,1
HA7	*Sequence error* (kesalahan urutan)	Low	0,1
HA8	*Information leaks* (kebocoran informasi)	Low	0,1
HA9	*Information modification* (modifikasi informasi)	Low	0,3
HA10	*Incorrect information entry* (salah memasukkan informasi)	Low	0,3
HA11	*Information degradation* (Degradasi informasi)	Low	0,1
HA12	*Configuration Error* (Kesalahan konfigurasi)	Low	0,3
HA13	*Disclosure of information* (Keterbukaan informasi)	Low	0,1
HA14	*Bug on software* (bug (kesalahan) software)	Low	0,3
HA15	*Defects in software maintenance or updating* (Cacat dalam pemeliharaan atau pembaruan perangkat lunak)	Low	0,1
HA16	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0,2
HA17	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0,2
HA18	*System failure due to exhaustion of resources* (Kegagalan sistem karena kehabisan sumber daya)	Low	0,1
HA19	*Staff shortage* (Kekurangan staf)	Medium	0,4
HD1	*Spying by a foreign state or a mafia (using important resources)* (Memata-matai oleh negara asing atau mafia)	Low	0,1
HD2	*Vandalism from outside: bullets or objects thrown from the street, etc.* (Vandalisme dari luar: peluru atau benda yang dilemparkan dari jalan, dll.)	Low	0,1

Kode	Jenis Ancaman	Probabilitas	Rerata Probabilitas
HD3	*Vandalism from inside: by people authorized within the premises (personnel, sub-contractor, etc.).* (Vandalisme dari dalam: oleh orang-orang yang diberi wewenang di dalam bangunan (personel, sub-kontraktor, dll.).	Low	0,1
HD4	*Terrorism: sabotage, explosives left close to sensitive premises* (Terorisme: sabotase, bahan peledak dekat dengan tempat sensitif)	Low	0,1
HD5	*Hardware theft* (Pencurian perangkat keras)	Low	0,1
HD6	*Network equipment theft* (Pencurian perangkat jaringan)	Low	0,1
HD7	*Malicious erasure of networking configurations* (Penghapusan berbahaya konfigurasi jaringan)	Low	0,1
HD8	*Malicious erasure of hardware configurations* (Penghapusan berbahaya konfigurasi perangkat keras)	Low	0,1
HD9	*Saturation of the network caused by a worm* (Kejenuhan jaringan disebabkan oleh worm)	Medium	0,4
HD10	*Malicious and repeated saturation of IT resources by a group of users* (Sumber daya TI berbahaya dan berulang oleh sekelompok pengguna)	Low	0,1
HD11	*Distorted data entry or fiddling of data* (Entri data terdistorsi atau mengutak-atik data)	Low	0,1
HD12	*Intentional erasure (direct or indirect), theft or destruction of program or data containers* (Penghapusan yang disengaja (langsung atau tidak langsung), pencurian atau penghancuran wadah program atau data)	Low	0,1
HD13	*Intended access to data or information and disclosure of information* (Dimaksudkan akses ke data atau informasi dan pengungkapan informasi)	Low	0,1
HD14	*Document or media theft* (Pencurian dokumen atau media)	Low	0,1
HD15	*Malicious erasure (directly or indirectly) of software on its storage* (Penghapusan berbahaya (langsung atau tidak langsung) dari perangkat lunak pada penyimpanannya)	Low	0,1
HD16	*Malicious modification (direct or indirect) of the functionalities of a program or of the operation of an office program (Excel, Access, etc)* Modifikasi berbahaya (langsung atau tidak langsung) dari fungsionalitas suatu program atau pengoperasian program perkantoran (Excel, Access, dll)	Low	0,1
HD17	*Illegal usage of software* (Penggunaan perangkat lunak secara ilegal)	Low	0,1
HD18	*Intrusion to system by third party whose contract with organization* (Intrusion ke sistem oleh pihak ketiga yang kontraknya dengan organisasi)	Low	0,1

Kode	Jenis Ancaman	Probabilitas	Rerata Probabilitas
HD19	*Malicious erasure of software configurations* (Penghapusan berbahaya konfigurasi perangkat lunak)	Low	0,1
HD20	*Absence or strike of IT operational personnel* (Tidak ada atau mogok personil operasional TI)	Low	0,1
HD21	*Masquerading of user identity* (Penyamaran identitas pengguna)	Low	0,1
HD22	*Abuse of access privileges* (Penyalahgunaan hak akses)	Low	0,3
HD23	*Software misuse* (Penyalahgunaan perangkat lunak)	Low	0,1
HD24	*Hardware misuse* (Penyalahgunaan perangkat keras)	Low	0,1
HD25	*Network misuse* (Penyalahgunaan jaringan)	Low	0,1
HD26	*Document misuse* (Penyalahgunaan dokumen)	Low	0,1
HD27	*Unauthorized access* (Akses yang tidak sah)	Medium	0,4
HD28	*Traffic analysis* (Analisis lalu lintas)	Low	0,1
HD29	*Eavesdropping* (Menguping)	Low	0,1
HD30	*Software manipulation* (Manipulasi perangkat lunak)	Low	0,2
HD31	*Denial of service* (Kegagalan layanan)	Low	0,1
HD32	*Extortion* (Pemerasan)	Low	0,1
HD33	*Social engineering* (Rekayasa sosial)	Low	0,1

Sumber: Rahmad et al., 2010, diolah

Langkah selanjutnya setelah menetapkan macam ancaman dan kerentanan beserta nilai dari probabilitas terjadi ancaman tersebut yaitu melakukan penghitungan Nilai ancaman tiap aset kritis. Proses penghitungan Nilai Ancaman tersebut dengan menggunakan rumusan sebagai berikut:

$$\textit{Nilai Ancaman (NT)} = \sum \textit{PO} \;/\; \sum \textit{Ancaman}$$

Dimana:

$\sum$ ***PO*** **:** Jumlah rerata probabilitas

$\sum$ ***Ancaman*** **:** Jumlah ancaman terhadap informasi pada suatu aset

Pada penelitian ini proses penghitungan nilai ancaman pada aset kritis dilakukan secara berkelompok dengan berdasar kesamaan jenis aset, type aset, fungsi aset dan tahun perolehan. Perhitungan detail tiap kelompok aset tersebut dapat dilihat pada lampiran 3.

Adapun rekapitulasi nilai ancaman aset dari perhitungan per kelompok aset tersebut dapat dilihat pada tabel 4.5 dibawah ini.

Tabel 4.5 Rekapitulasi nilai ancaman aset dari perhitungan per kelompok aset

No	Nama Aset	Merek / Type	Tahun Perolehan	Deskripsi Aset	Nilai NT
1	SI Akademik				0.265
2	SIM Rencana Belanja Anggaran (SIM RBA)				0.265
3	SIM Keuangan				0.265
4	SI Monitoring Pendapatan ITS (SIMONDITS)				0.265
5	Host-to-host App				0.265
6	SIM Kepegawaian				0.265
7	Sistem Informasi Pelaporan Data				0.265
8	Executive Reporting				0.265
9	Single Sign On (SSO) App				0.256
10	Modulas Monitoring System	Modul	2009	Network Backbone	0.367
11	Fiber Optic Operating	GE	2010	Network Backbone	0.367
12	Interface Network	CISCO	2010	Network Backbone	0.367
13	Paralel Control Network	CISCO	2010	Network Backbone	0.367
14	Internet Network	CISCO	2010	Network Backbone	0.367
15	Server	HPE DL580 Gen9 CTO SVR	2017	OLTP server dan OLAP Server	0.26

No	Nama Aset	Merek / Type	Tahun Perolehan	Deskripsi Aset	Nilai NT
16	Server	HPE DL380 Gen9 CTO Derver	2017	VMWare 65 Server	0.26
17	Server	HPE MSA 2040 SAN	2017	Database Storage	0.26
18	Server	HP / PROLIANT ML150	2005	Server Aplikasi Unit	0.294
19	Server	Advance Server SUN X4100	2009	Data Center	0.294
20	Server	HP PROLIANT DL380G6	2010	Server Aplikasi Unit	0.294
21	Server	HPPROLIANT DL 145 R G3,AMD OPTERON2.2 GHZ.MON 15	2010	Server Aplikasi Unit	0.294
22	Server	UPS ICA RN 3200C	2011	UPS Server	0.294
23	Server	HP DL580R07 CTO Chassis (Database)	2011	Database Server	0.294
24	Server	HP DL380E	2012	HyperV Server	0.294
25	Server	HP/Proliant DL380G7	2012	Proxmox VE Server	0.294
26	Server	HP/DL580	2014	VMWare 22 Server	0.294
27	Server	DELL/PowerEdge R230	2016	Hosting zeus Server	0.26
28	Server	HPE/Proliant DL580 Gen10	2018	Proxmox VE Server	0.26
29	Server	HPE/ProLiant DL380 Gen10	2018	Proxmox VE Server	0.26
30	Wireless Access Point	Cisco/AIR-CAP2702I-F	2016	Distributor Wireless AP	0.25
31	Wireless Access Point	CISCO Aironet 1852E	2017	Distributor Wireless AP	0.25

No	Nama Aset	Merek / Type	Tahun Perolehan	Deskripsi Aset	Nilai NT
32	Wireless Access Point	CISCO Aironet 3802E	2017	Distributor Wireless AP	0.25
33	Firewall	Barracuda 641 ADC	2017	Network Firewall	0.246
34	Firewall	Firewall Cisco ASA 5585-X	2011	Network Firewall	0.246
35	Router	Gigabit Router Cisco 3945	2011	Main Router	0.233
36	Router	CISCO 7606 S	2012	Core Router	0.233
37	Router	Cisco ASR 1002X	2016	Core BGP router	0.233
38	Router	RB 1100 HX2	2013	Internet Access	0.233
39	Auto Switch/Data Switch	CISCO 4900	2010	Access Switch	0.233
40	Auto Switch/Data Switch	CISCO 3560	2010	Access Switch	0.233
41	Auto Switch/Data Switch	HPE 1820	2018	Access Switch	0.233
42	Auto Switch/Data Switch	CISCO 3560	2018	Access Switch	0.233
43	Switch	Nexus N9K-C93120TX bundle 2pcs	2017	Database Data Switch	0.245
44	Switch	Cisco Catalyst 3560X 24 Port	2011	Access Switch	0.233
45	Switch	TP-Link	2013	Access Switch	0.233
46	Switch	Cisco/WS-C4900M	2014	Distributor Switch	0.233
47	Switch	HP 1820	2016	Access Switch	0.233

No	Nama Aset	Merek / Type	Tahun Perolehan	Deskripsi Aset	Nilai NT
48	Switch	HPE/FlexFabric 5940	2018	Datacentre Access Switch	0.233
49	Switch	Huawei 12700	2016	Core Switch	0.233
50	Switch	Cisco 6500	2016	Core Switch	0.233
51	Switch	Cisco 7700	2016	Core Switch	0.233
52	Storage Modul Disk (Peralatan Mainframe)	SAN/Storage	2012	Data Centre	0.317
53	Storage Modul Disk (Peralatan Mainframe)	Hitachi/HUS110	2014	Data Centre	0.317
54	Stabilizer/UPS	UPS Protekta	2009	UPS Server	0.3
55	Uninterupted Power Supply (UPS)	Rackmounted TCL3300	2012	UPS Server	0.3
56	Genset	CATERPILLAR ECW00427	2015		0.3
57	A.C. Split	Type CS-D43DB4H5 (5 HP)	2010	Data Center AC	0.333
58	A.C. Split	Panasonic	2013	Data Center AC	0.333
59	A.C. Split	Daikin STNE	2016	Data Center AC	0.333
60	CCTV - Camera Control Television System	Hikvision	2018	Kamera Pengaman	0.333
61	Alat Sidik Jari	FInger Prnt	2014	Pengaman Pintu	0.333

4.3 Analisis Dampak Bisnis (Business Impact Analysis)

Analisis Dampak Bisnis atau yang biasa disebut dengan istilah BIA (*Business Impact Analysis*) adalah gambaran seberapa tahan proses bisnis di dalam organisasi berjalan jika informasi yang dimiliki terganggu. Analisis dampak bisnis dilakukan dengan menentukan skala nilai BIA, sebagaimana dicontohkan pada tabel 4.6 berikut:

Tabel 4.6 Contoh skala nilai BIA

Batas Toleransi Gangguan	***Keterangan***	***Nilai Skala***
< dari 1 minggu	*Not Critical*	0-20
1 hari s/d 2 hari	*Minor Critical*	21-40
< 1 hari	*Mayor Critical*	41-60
< 12 Jam	*High Critical*	61-80
< 1 Jam	*Very High Critical*	81-100

Sumber : (Sarno and Iffano, 2009)

Dari skala yang telah dicontohkan pada tabel diatas maka dilakukan penilaian pada aset kritis yang dikelola oleh DPTSI.

Adapun hasil dari nilai BIA pada aset kritis tersebut dapat dilihat pada tabel 4.7 berikut ini:

Tabel 4.7 Penilaian BIA pada Aset kritis.

No	Nama Aset	Merek / Type	Deskripsi Aset	Dampak *(impact)*	Nilai BIA
1	SI Akademik			Layanan Informasi akademik terhenti	65
2	SIM Rencana Belanja Anggaran (SIM RBA)			Rencana belanja tertunda	25
3	SIM Keuangan			keuangan tidak terlaporkan	80
4	SI Monitoring Pendapatan ITS (SIMONDITS)			pendapatan tidak terpantau	25
5	Host-to-host App			layanan tranfer keuangan gagal	60
6	SIM Kepegawaian			Informasi kepegawaian tidak terproses	30
7	Sistem Informasi Pelaporan Data			Informasi data ITS tidak terbaca	25
8	Executive Reporting			Laporan summary ITS tidak terbaca	40
9	Single Sign On (SSO) App			akses ke semua SIM putus	95
10	Modulas Monitoring System	Modul	Network Backbone	Jaringan terputus total	80
11	Fiber Optic Operating	GE	Network Backbone	Jaringan terputus total	80
12	Interface Network	CISCO	Network Backbone	Jaringan terputus total	80
13	Paralel Control Network	CISCO	Network Backbone	Jaringan terputus total	80
14	Internet Network	CISCO	Network Backbone	Jaringan terputus total	80
15	Server	HPE DL580 Gen9 CTO SVR	OLTP server dan OLAP Server	Analisa data online terputus	40

No	Nama Aset	Merek / Type	Deskripsi Aset	Dampak *(impact)*	Nilai BIA
16	Server	HPE DL380 Gen9 CTO Derver	VMWare 65 Server	Transaksi dengan SIM terhenti	75
17	Server	HPE MSA 2040 SAN	Database Storage	Data tidak dapat diakses	80
18	Server	HP / PROLIANT ML150	Server Aplikasi Unit	Aplikasi unit tidak berfungsi	60
19	Server	Advance Server SUN X4100	Data Center	Data tidak dapat diakses	80
20	Server	HP PROLIANT DL380G6	Server Aplikasi Unit	Aplikasi unit tidak berfungsi	60
21	Server	HPPROLIANT DL 145 R G3,AMD OPTERON2.2 GHZ.MON 15	Server Aplikasi Unit	Aplikasi unit tidak berfungsi	60
22	Server	UPS ICA RN 3200C	UPS Server	Server kekurangan stok listrik	25
23	Server	HP DL580R07 CTO Chassis (Database)	Database Server	Data tidak dapat diakses	80
24	Server	HP DL380E	HyperV Server	Transaksi dengan SIM terhenti	75
25	Server	HP/Proliant DL380G7	Proxmox VE Server	Transaksi dengan SIM terhenti	75
26	Server	HP/DL580	VMWare 22 Server	Transaksi dengan SIM terhenti	75
27	Server	DELL/PowerEdge R230	Hosting zeus Server	Transaksi dengan SIM terhenti	75
28	Server	HPE/Proliant DL580 Gen10	Proxmox VE Server	Transaksi dengan SIM terhenti	75
29	Server	HPE/ProLiant DL380 Gen10	Proxmox VE Server	Transaksi dengan SIM terhenti	75
30	Wireless Access Point	Cisco/AIR-CAP2702I-F	Distributor Wireless AP	Komunikais data antar unit mati	60
31	Wireless Access Point	CISCO Aironet 1852E	Distributor Wireless AP	Komunikais data antar unit mati	60

No	Nama Aset	Merek / Type	Deskripsi Aset	Dampak *(impact)*	Nilai BIA
32	Wireless Access Point	CISCO Aironet 3802E	Distributor Wireless AP	Komunikais data antar unit mati	60
33	Firewall	Barracuda 641 ADC	Network Firewall	Server dapat diserang hacker	70
34	Firewall	Firewall Cisco ASA 5585-X	Network Firewall	Server dapat diserang hacker	70
35	Router	Gigabit Router Cisco 3945	Main Router	Komunikais data antar unit mati	65
36	Router	CISCO 7606 S	Core Router	Komunikais data antar unit mati	65
37	Router	Cisco ASR 1002X	Core BGP router	Komunikais data antar unit mati	65
38	Router	RB 1100 HX2	Internet Access	Akses internet putus	40
39	Auto Switch/Data Switch	CISCO 4900	Access Switch	Komunikais data antar unit mati	60
40	Auto Switch/Data Switch	CISCO 3560	Access Switch	Komunikais data antar unit mati	60
41	Auto Switch/Data Switch	HPE 1820	Access Switch	Komunikais data antar unit mati	60
42	Auto Switch/Data Switch	CISCO 3560	Access Switch	Komunikais data antar unit mati	60
43	Switch	Nexus N9K-C93120TX bundle 2pcs	Database Data Switch	Data tidak dapat diakses	80
44	Switch	Cisco Catalyst 3560X 24 Port	Access Switch	Komunikais data antar unit mati	60
45	Switch	TP-Link	Access Switch	Komunikais data antar unit mati	60
46	Switch	Cisco/WS-C4900M	Distributor Switch	Komunikais data antar unit mati	70
47	Switch	HP 1820	Access Switch	Komunikais data antar unit mati	60

No	Nama Aset	Merek / Type	Deskripsi Aset	Dampak *(impact)*	Nilai BIA
48	Switch	HPE/FlexFabric 5940	Datacentre Access Switch	Data tidak dapat diakses	80
49	Switch	Huawei 12700	Core Switch	Komunikais data antar unit mati	80
50	Switch	Cisco 6500	Core Switch	Komunikais data antar unit mati	80
51	Switch	Cisco 7700	Core Switch	Komunikais data antar unit mati	80
52	Storage Modul Disk (Peralatan Mainframe)	SAN/Storage	Data Centre	Data tidak dapat diakses	80
53	Storage Modul Disk (Peralatan Mainframe)	Hitachi/HUS110	Data Centre	Data tidak dapat diakses	80
54	Stabilizer/UPS	UPS Protekta	UPS Server	Server kekurangan stok listrik	25
55	Uninterupted Power Supply (UPS)	Rackmounted TCL3300	UPS Server	Server kekurangan stok listrik	25
56	Genset	CATERPILLAR ECW00427		Server kekurangan stok listrik	25
57	A.C. Split	Type CS-D43DB4H5 (5 HP)	Data Center AC	Server overheat trus mati	70
58	A.C. Split	Panasonic	Data Center AC	Server overheat trus mati	70
59	A.C. Split	Daikin STNE	Data Center AC	Server overheat trus mati	70
60	CCTV - Camera Control Television System	Hikvision	Kamera Pengaman	Keamanan tidak terpantau	50
61	Alat Sidik Jari	FInger Prnt	Pengaman Pintu	Tidak dapat masuk R. server	75

4.4 Penghitungan Nilai Risiko dan Level Risiko

Berdasar hasil dari langkah-langkah sebelumnya, maka tindakan berikutnya yaitu melakukan penghitungan Nilai Risiko. Penghitungan ini dilakukan dengan menggunakan Nilai Aset, Nilai Ancaman dan Nilai BIA. Adapun formulasi dari penghitungan Nilai risiko adalah sebagai berikut:

Nilai Risiko (Risk Value) =(NA x BIA x NT) / 10

Dimana:

- NA : Nilai Aset (*Asset Value*)
- BIA : Nilai Dampak Bisnis (*Business Impact Analysis*)
- NT : Nilai Ancaman (*Threat Value*)

Setelah nilai risiko diketahui maka tindakan selanjutnya adalah mencari level risiko dari aset tersebut. Penentuan level risiko ini dapat dibantu dengan menggunakan matriks level risiko sebagaimana terlihat pada tabel 2.10 pada bab sebelumnya.

Dengan menggunakan rumusan diatas maka didapatkan tabel hasil penilaian risiko dan level risiko pada Aset sebagaimana berikut ini.

Tabel 4.8 Hasil penilaian risiko dan level risiko pada aset DPTSI

No	Nama Aset	Merek / Type	Nilai NA	Nilai BIA	Nilai NT	Nilai Risiko	Level Risiko
1	SI Akademik		10	65	0.27	17.23	Medium
2	SIM Rencana Belanja Anggaran (SIM RBA)		7	25	0.27	4.64	Low
3	SIM Keuangan		9	80	0.27	19.08	Medium
4	SI Monitoring Pendapatan ITS (SIMONDITS)		9	25	0.27	5.96	Low
5	Host-to-host App		9	60	0.27	14.31	Medium
6	SIM Kepegawaian		8	30	0.27	6.36	Low
7	Sistem Informasi Pelaporan Data		7	25	0.27	4.64	Low
8	Executive Reporting		7	40	0.27	7.42	Low
9	Single Sign On (SSO) App		12	95	0.26	29.21	Medium
10	Modulas Monitoring System	Modul	7	80	0.37	20.53	Medium
11	Fiber Optic Operating	GE	11	80	0.37	32.27	Medium
12	Interface Network	CISCO	10	80	0.37	29.33	Medium
13	Paralel Control Network	CISCO	10	80	0.37	29.33	Medium
14	Internet Network	CISCO	10	80	0.37	29.33	Medium
15	Server	HPE DL580 Gen9 CTO SVR	11	40	0.26	11.44	Medium

No	Nama Aset	Merek / Type	Nilai NA	Nilai BIA	Nilai NT	Nilai Risiko	Level Risiko
16	Server	HPE DL380 Gen9 CTO Derver	11	75	0.26	21.45	Medium
17	Server	HPE MSA 2040 SAN	11	80	0.26	22.88	Medium
18	Server	HP / PROLIANT ML150	11	60	0.29	19.39	Medium
19	Server	Advance Server SUN X4100	11	80	0.29	25.85	Medium
20	Server	HP PROLIANT DL380G6	11	60	0.29	19.39	Medium
21	Server	HPPROLIANT DL 145 R G3,AMD OPTERON2.2 GHZ.MON 15	11	60	0.29	19.39	Medium
22	Server	UPS ICA RN 3200C	11	25	0.29	8.08	Low
23	Server	HP DL580R07 CTO Chassis (Database)	11	80	0.29	25.85	Medium
24	Server	HP DL380E	11	75	0.29	24.23	Medium
25	Server	HP/Proliant DL380G7	11	75	0.29	24.23	Medium
26	Server	HP/DL580	11	75	0.29	24.23	Medium
27	Server	DELL/PowerEdge R230	11	75	0.26	21.45	Medium
28	Server	HPE/Proliant DL580 Gen10	11	75	0.26	21.45	Medium
29	Server	HPE/ProLiant DL380 Gen10	11	75	0.26	21.45	Medium
30	Wireless Access Point	Cisco/AIR-CAP2702I-F	8	60	0.25	12.00	Medium

No	Nama Aset	Merek / Type	Nilai NA	Nilai BIA	Nilai NT	Nilai Risiko	Level Risiko
31	Wireless Access Point	CISCO Aironet 1852E	8	60	0.25	12.00	Medium
32	Wireless Access Point	CISCO Aironet 3802E	8	60	0.25	12.00	Medium
33	Firewall	Barracuda 641 ADC	10	70	0.25	17.23	Medium
34	Firewall	Firewall Cisco ASA 5585-X	10	70	0.25	17.23	Medium
35	Router	Gigabit Router Cisco 3945	9	65	0.23	13.65	Medium
36	Router	CISCO 7606 S	9	65	0.23	13.65	Medium
37	Router	Cisco ASR 1002X	10	65	0.23	15.17	Medium
38	Router	RB 1100 HX2	10	40	0.23	9.33	Low
39	Auto Switch/Data Switch	CISCO 4900	9	60	0.23	12.60	Medium
40	Auto Switch/Data Switch	CISCO 3560	9	60	0.23	12.60	Medium
41	Auto Switch/Data Switch	HPE 1820	9	60	0.23	12.60	Medium
42	Auto Switch/Data Switch	CISCO 3560	9	60	0.23	12.60	Medium
43	Switch	Nexus N9K-C93120TX bundle 2pcs	10	80	0.25	19.64	Medium
44	Switch	Cisco Catalyst 3560X 24 Port	9	60	0.23	12.60	Medium
45	Switch	TP-Link	9	60	0.23	12.60	Medium
46	Switch	Cisco/WS-C4900M	10	70	0.23	16.33	Medium

No	Nama Aset	Merek / Type	Nilai NA	Nilai BIA	Nilai NT	Nilai Risiko	Level Risiko
47	Switch	HP 1820	9	60	0.23	12.60	Medium
48	Switch	HPE/FlexFabric 5940	10	80	0.23	18.67	Medium
49	Switch	Huawei 12700	10	80	0.23	18.67	Medium
50	Switch	Cisco 6500	10	80	0.23	18.67	Medium
51	Switch	Cisco 7700	10	80	0.23	18.67	Medium
52	Storage Modul Disk (Peralatan Mainframe)	SAN/Storage	11	80	0.32	27.87	Medium
53	Storage Modul Disk (Peralatan Mainframe)	Hitachi/HUS110	11	80	0.32	27.87	Medium
54	Stabilizer/UPS	UPS Protekta	7	25	0.30	5.25	Low
55	Uninterupted Power Supply (UPS)	Rackmounted TCL3300	7	25	0.30	5.25	Low
56	Genset	CATERPILLAR ECW00427	7	25	0.30	5.25	Low
57	A.C. Split	Type CS-D43DB4H5 (5 HP)	9	70	0.33	21.00	Medium
58	A.C. Split	Panasonic	9	70	0.33	21.00	Medium
59	A.C. Split	Daikin STNE	9	70	0.33	21.00	Medium
60	CCTV - Camera Control Television System	Hikvision	8	50	0.33	13.33	Medium
61	Alat Sidik Jari	FInger Prnt	11	75	0.33	27.50	Medium

4.5 Evaluasi dan Penanganan Risiko

Langkah yang harus dilakukan oleh organisasi selanjutnya dalam penanganan risiko keamanan informasi yaitu menentukan level penerimaan risiko. Level ini berfungsi sebagai kontrol organisasi untuk dapat menentukan sejauh mana suatu risiko keamanan informasi dapat diterima oleh organisasi atau bahkan risiko tersebut harus dilimpahkan ke pihak ketiga sebagai jaminan tetap berjalannya sistem dan menjaga keamanan informasi yang dimiliki. Adapun kriteria level penerimaan risiko dapat dikategorikan sebagai berikut:

a. Risiko Diterima (*risk acceptance*)

   Organisasi menerima risiko yang terjadi dengan segala dampaknya dan proses bisnis organisasi berlangsung terus.

b. Risiko direduksi (*risk reduction / mitigate*)

   Organisasi menerima risiko tetapi direduksi dengan menggunakan Kontrol keamanan sampai pada level yang dapat diterima oleh organisasi.

c. Risiko dihindari atau ditolak (*risk avoidance*)

   Organisasi menghindari risiko yang terjadi dengan cara menghilangkan penyebab timbulnya risiko atau organisasi menghentikan aktivitasnya jika gejala risiko muncul (seperti: mematikan server, memutus koneksi jaringan dan lain-lain).

d. Risiko dialihkan ke pihak ketiga (*risk transfer*)

   Organisasi menerima risiko yang ada dengan cara mengalihkan kepada pihak ketiga untuk mendapatkan penggantian atau kompensasi dari pihak ketiga tersebut (seperti: asuransi, vendor dan lain-lain).

Sebagaimana dijelaskan pada bab 2, penerimaan risiko dapat menggunakan tabel dengan matriks yang menghubungkan antar 3 (tiga) variabel yang ada, yaitu:

- Probabilitas Ancaman (*threat probability*).
- Biaya Pemulihan (*recovery cost*) akibat dampak dari penerimaan risiko.
- Biaya Transfer risiko (*risk transfer cost*) kepada pihak ketiga.

Adapun tabel penerimaan risiko dapat dilihat sebagai berikut:

Tabel 4.9 Tabel Penerimaan Risiko

PA	BP	BR	Nilai	Kriteria
LOW	LOW	HIGH	LOW	Risk Acceptance
MED	LOW	HIGH	LOW	Risk Acceptance
HIGH	LOW	HIGH	LOW	Risk Acceptance
LOW	MED	MED	LOW	Risk Reduction / Mitigate
MED	MED	MED	MED	Risk Reduction / Mitigate
HIGH	MED	MED	MED	Risk Avoid
LOW	HIGH	LOW	LOW	Risk Transfer
MED	HIGH	LOW	LOW	Risk Transfer
HIGH	HIGH	LOW	LOW	Risk Transfer

Sumber: Sarno, 2009

Maka dengan demikian evakuasi penerimaan yang dilakukan terhadap risiko aset informasi DPTSI dapat dilihat pada tabel 4.9.

Tabel 4.10 Penerimaan Risiko pada aset kritis DPTSI

No	Nama Aset	Merek / Type	Level Risiko	Peneriman Risiko
1	SI Akademik		Medium	Risk Reduction
2	SIM Rencana Belanja Anggaran (SIM RBA)		Low	Risk Acceptance
3	SIM Keuangan		Medium	Risk Reduction
4	SI Monitoring Pendapatan ITS (SIMONDITS)		Low	Risk Acceptance
5	Host-to-host App		Medium	Risk Reduction
6	SIM Kepegawaian		Low	Risk Acceptance
7	Sistem Informasi Pelaporan Data		Low	Risk Acceptance
8	Executive Reporting		Low	Risk Acceptance
9	Single Sign On (SSO) App		Medium	Risk Reduction
10	Modulas Monitoring System	Modul	Medium	Risk Reduction
11	Fiber Optic Operating	GE	Medium	Risk Reduction
12	Interface Network	CISCO	Medium	Risk Reduction
13	Paralel Control Network	CISCO	Medium	Risk Reduction
14	Internet Network	CISCO	Medium	Risk Reduction
15	Server	HPE DL580 Gen9 CTO SVR	Medium	Risk Reduction

No	Nama Aset	Merek / Type	Level Risiko	Peneriman Risiko
16	Server	HPE DL380 Gen9 CTO Derver	Medium	Risk Reduction
17	Server	HPE MSA 2040 SAN	Medium	Risk Reduction
18	Server	HP / PROLIANT ML150	Medium	Risk Reduction
19	Server	Advance Server SUN X4100	Medium	Risk Reduction
20	Server	HP PROLIANT DL380G6	Medium	Risk Reduction
21	Server	HPPROLIANT DL 145 R G3,AMD OPTERON2.2 GHZ.MON 15	Medium	Risk Reduction
22	Server	UPS ICA RN 3200C	Low	Risk Acceptance
23	Server	HP DL580R07 CTO Chassis (Database)	Medium	Risk Reduction
24	Server	HP DL380E	Medium	Risk Reduction
25	Server	HP/Proliant DL380G7	Medium	Risk Reduction
26	Server	HP/DL580	Medium	Risk Reduction
27	Server	DELL/PowerEdge R230	Medium	Risk Reduction
28	Server	HPE/Proliant DL580 Gen10	Medium	Risk Reduction
29	Server	HPE/ProLiant DL380 Gen10	Medium	Risk Reduction
30	Wireless Access Point	Cisco/AIR-CAP2702I-F	Medium	Risk Reduction
31	Wireless Access Point	CISCO Aironet 1852E	Medium	Risk Reduction
32	Wireless Access Point	CISCO Aironet 3802E	Medium	Risk Reduction
33	Firewall	Barracuda 641 ADC	Medium	Risk Reduction
34	Firewall	Firewall Cisco ASA 5585-X	Medium	Risk Reduction
35	Router	Gigabit Router Cisco 3945	Medium	Risk Reduction
36	Router	CISCO 7606 S	Medium	Risk Reduction
37	Router	Cisco ASR 1002X	Medium	Risk Reduction
38	Router	RB 1100 HX2	Low	Risk Acceptance
39	Auto Switch/Data Switch	CISCO 4900	Medium	Risk Reduction
40	Auto Switch/Data Switch	CISCO 3560	Medium	Risk Reduction
41	Auto Switch/Data Switch	HPE 1820	Medium	Risk Reduction
42	Auto Switch/Data Switch	CISCO 3560	Medium	Risk Reduction
43	Switch	Nexus N9K-C93120TX bundle 2pcs	Medium	Risk Reduction

No	Nama Aset	Merek / Type	Level Risiko	Peneriman Risiko
44	Switch	Cisco Catalyst 3560X 24 Port	Medium	Risk Reduction
45	Switch	TP-Link	Medium	Risk Reduction
46	Switch	Cisco/WS-C4900M	Medium	Risk Reduction
47	Switch	HP 1820	Medium	Risk Reduction
48	Switch	HPE/FlexFabric 5940	Medium	Risk Reduction
49	Switch	Huawei 12700	Medium	Risk Reduction
50	Switch	Cisco 6500	Medium	Risk Reduction
51	Switch	Cisco 7700	Medium	Risk Reduction
52	Storage Modul Disk (Peralatan Mainframe)	SAN/Storage	Medium	Risk Reduction
53	Storage Modul Disk (Peralatan Mainframe)	Hitachi/HUS110	Medium	Risk Reduction
54	Stabilizer/UPS	UPS Protekta	Low	Risk Acceptance
55	Uninterupted Power Supply (UPS)	Rackmounted TCL3300	Low	Risk Acceptance
56	Genset	CATERPILLAR ECW00427	Low	Risk Acceptance
57	A.C. Split	Type CS-D43DB4H5 (5 HP)	Medium	Risk Reduction
58	A.C. Split	Panasonic	Medium	Risk Reduction
59	A.C. Split	Daikin STNE	Medium	Risk Reduction
60	CCTV - Camera Control Television System	Hikvision	Medium	Risk Reduction
61	Alat Sidik Jari	FInger Prnt	Medium	Risk Reduction

4.6 Pemetaan Risiko dengan Kontrol ISO27001:2013

Pada tahap ini akan dilakukan penanganan (kontrol) terhadap risiko yang dihadapi oleh tiap-tiap aset. Kontrol yang digunakan untuk mengendalikan dan mereduksi risiko keamanan menggunakan standart ISO/IEC 27001:2013. Sebagaimana disebutkan pada bab 2, bahwa pada ISO 27001:2013 terdapat 14 grup kontrol dan 35 buah sasaran pengendalian.

Pada proses pemetaan kontrol ini, dilakukan pengelompokan Aset berdasarkan jenis aset dan fungsi aset informasi. Berikut adalah tabel pemetaan kontrol ISO 27001:2013 terhadap risiko aset informasi yang ada pada DPTSI.

Tabel 4.11 Pemetaan Resiko Keamanan Aset terhadap Kontrol ISO 27001:2013

No	Jenis Aset / Fungsi Aset	Level Risiko	Peneriman Risiko	Kontrol ISO 27001
1	Sistem Informasi	Medium	Risk Reduction	A.5.1.1; A.6.1.1; A.6.1.3; A.7.2.2; A.8.1.1; A.9.1.1; A.9.2.1; A.9.2.2; A.9.2.6; A.9.4.1; A.9.4.2; A.9.4.3; A.9.4.5; A.10.1.1; A.12.1.1; A.12.2.1; A.12.3.1; A.12.4.1; A.14.1.2; A.14.2.1; A.16.1.2; A.16.1.3
2	Back Bone (FO) Network	Medium	Risk Reduction	A.5.1.1; A.6.1.1; A.6.1.3; A.8.1.1; A.11.2.1; A.11.2.3; A.13.1.1; A.15.1.1; A.15.2.1
3	Server	Medium	Risk Reduction	A.5.11; A.6.1.1; A.7.2.2; A.8.1.1; A.8.13; A.9.1.1; A.9.1.2; A.9.2.1; A.9.2.2; A.9.2.3; A.9.2.5; A.9.2.6; A.9.4.1; A.9.4.2; A.9.4.3; A.11.1.1; A.11.1.2; A.11.1.3; A.11.1.4; A.11.2.1; A.11.2.2; A.11.2.4; A.12.11; A.12.3.1; A.12.4.1; A.12.4.2; A.12.4.3; A.12.5.1;
4	Wireless Access Point	Medium	Risk Reduction	A.5.1.1; A.8.1.1; A.11.2.1; A.11.2.2; A.11.2.4; A.12.1.1
5	Firewall	Medium	Risk Reduction	A.5.1.1; A.8.1.1; A.11.1.1; A.11.1.2; A.11.2.1; A.11.2.2; A.11.2.4; A.12.1.1
6	Router	Medium	Risk Reduction	A.5.1.1; A.8.1.1; A.11.1.1; A.11.1.2; A.11.2.1; A.11.2.2; A.11.2.4; A.12.1.1
7	Switch	Medium	Risk Reduction	A.5.1.1; A.8.1.1; A.11.1.1; A.11.1.2; A.11.2.1; A.11.2.2; A.11.2.4; A.12.1.1
8	Storage Modul Disk	Medium	Risk Reduction	A.5.1.1; A.8.1.1; A.11.1.1; A.11.1.2; A.11.2.1; A.11.2.2; A.11.2.4; A.12.1.1; A.12.3.1
9	Uninterupted Power Supply (UPS)	Low	Risk Acceptance	A.5.1.1; A.8.1.1; A.11.2.1; A.11.2.2; A.11.2.4; A.12.1.1
10	Genset	Low	Risk Acceptance	A.5.1.1; A.8.1.1; A.11.1.1; A.11.1.2; A.11.2.1; A.11.2.2; A.11.2.4; A.12.1.1
11	A.C. Split	Medium	Risk Reduction	A.5.1.1; A.8.1.1; A.11.2.1; A.11.2.2; A.11.2.4; A.12.1.1
12	CCTV - Camera Control Television System	Medium	Risk Reduction	A.5.1.1; A.8.1.1; A.11.2.1; A.11.2.2; A.11.2.4; A.12.1.1
13	Alat Sidik Jari	Medium	Risk Reduction	A.5.1.1; A.8.1.1; A.11.2.1; A.11.2.2; A.11.2.4; A.12.1.1

Penjelasan pengendalian untuk masing-masing kontrol ISO 27001, yang telah dipetakan terhadap aset kritis tersebut dapat dilihat pada tabel 4.12 dibawah.

Selanjutnya dibuatlah tabel rekomendasi kebijakan yang dibuat berdasar kejadian ancaman keamanan informasi yang pernah terjadi / dialami oleh DPTSI ITS yang berdampak cukup kritis pada operasional organisasi. Tabel rekomendasi kebijakan terseut dapat dilihat pada tabel 4.13 dibawah.

Tabel 4.12 Pengendalian Risiko pada Aset sesuai Kontrol ISO 27001:2013

No	Jenis Aset / Fungsi Aset	Penerimaan Risiko	Kontrol ISO 27001	Pengendalian
1	Sistem Informasi	Risk Reduction	A.5.1.1; Kebijakan keamanan informasi	Dokumen kebijakan keamanan informasi harus disahkan oleh manajemen dan dipublikasikan serta dikomunikasikan kepada semua karyawan dan pihak-pihak lain yang relevan.
			A.6.1.1; Tugas dan tanggung jawab keamanan informasi	Semua tanggung jawab keamanan informasi harus ditetapkan dan diinformasikan.
			A.6.1.3; Kontak dengan pihak berwenang	Kontak dengan pihak berwenang yang relevan harus dipelihara.
			A.7.2.2; Kepedulian, pendidikan dan pelatihan keamanan informasi	Setiap pegawai dan kontraktor harus secara berkala mendapat pelatihan yang cukup tentang kepedulian, kebijakan dan prosedur yang berlaku sesuai dengan pekerjaan masing-masing.
			A.8.1.1; Inventarisasi aset	Aset-aset yang berhubungan dengan perangkat pemrosesan informasi harus diidentifikasi dengan jelas dan inventarisasi semua aset penting harus dicatat dan dipelihara.
			A.9.1.1; Kebijakan kontrol akses	Kebijakan kontrol akses harus ditetapkan, didokumentasikan dan dikaji ulang berdasarkan ketentuan bisnis dan persyaratan keamanan informasi.
			A.9.2.1; Akses ke jaringan dan layanan jaringan	User hanya dapat mengakses jaringan dan layanan jaringan yang telah secara spesifik diberikan kewenangan.
			A.9.2.2; Penyediaan user access	Proses penyediaan user access harus diimplementasikan untuk pemberian atau pembatalan hak akses terhadap semua jenis user.
			A.9.2.6; Penghapusan atau Penyesuaian Hak Akses	Proses penghapusan atau penutupan hak Akses untuk user yang sudah tidak berkepentingan.
			A.9.4.1; Pembatasan akses informasi	Akses terhadap informasi dan fungsi sistem aplikasi harus dibatasi sesuai dengan kebijakan kontrol akses.
			A.9.4.2; Prosedur log-on yang aman	Apabila disyaratkan kebijakan kontrol akses, akses ke sistem dan aplikasi harus dikendalikan dengan prosedur log-on.
			A.9.4.3; Sistem manajemen password	Manajemen password harus interaktif dan menjamin kualitas password.
			A.9.4.5; Kontrol akses terhadap program source code	Akses ke program source code harus dibatasi.

No	Jenis Aset / Fungsi Aset	Penerimaan Risiko	Kontrol ISO 27001	Pengendalian
			A.10.1.1; Kebijakan penggunaan kontrol kriptografi	Kebijakan penggunaan kontrol kriptografi untuk memproteksi informasi harus dikembangkan dan diimplementasikan.
			A.12.1.1; Prosedur operasi yang terdokumentasi	Prosedur pengoperasian harus didokumentasikan, dipelihara dan tersedia untuk semua user yang membutuhkan prosedur tersebut.
			A.12.2.1; Kontrol malware	Kontrol yang bersifat pendeteksian, pencegahan dan pemulihan agar terlindung dari malware untuk memberikan kesadaran user harus diterapkan.
			A.12.3.1; Back-up informasi	Back-up copy informasi, software dan sistem gambar (system images) harus dilakukan dan diuji secara berkala sesuai dengan kebijakan back-up yang telah ditetapkan.
			A.12.4.1; Kegiatan log	Kegiatan log yang merekam aktivitas user, kelainan-kelainan, kesalahan dan kejadian keamanan informasi harus dibuat, disimpan dan di-review secara berkala.
			A.14.1.2; Pengamanan layanan aplikasi pada jaringan publik	Informasi yang melewati jaringan publik harus dilindungi dari aktivitas penipuan, perselisihan kontrak, pengungkapan yang tidak sah dan modifikasi.
			A.14.2.1; Kebijakan pengembangan yang aman	Aturan pengembangan software dan sistem harus ditetapkan dan diterapkan untuk proses pengembangan dalam organisasi.
			A.16.1.2; Pelaporan kejadian keamanan informasi	Kejadian keamanan informasi harus dilaporkan kepada manajemen yang tepat secepat mungkin.
			A.16.1.3; Pelaporan kelemahan keamanan	Semua karyawan dan kontraktor yang menggunakan sistem informasi milik organisasi diwajibkan mencatat dan melaporkan setiap kelemahan keamanan yang diamati atau dicurigai dalam sistem atau layanan.
2	Back Bone (FO) Network	Risk Reduction	A.5.1.1; Kebijakan keamanan informasi	Dokumen kebijakan keamanan informasi harus disahkan oleh manajemen dan dipublikasikan serta dikomunikasikan kepada semua karyawan dan pihak-pihak lain yang relevan.
			A.6.1.1; Tugas dan tanggung jawab keamanan informasi	Semua tanggung jawab keamanan informasi harus ditetapkan dan diinformasikan.
			A.6.1.3; Kontak dengan pihak berwenang	Kontak dengan pihak berwenang yang relevan harus dipelihara.
			A.8.1.1; Inventarisasi aset	Aset-aset yang berhubungan dengan perangkat pemrosesan informasi harus diidentifikasi dengan jelas dan inventarisasi semua aset penting harus dicatat dan dipelihara.

No	Jenis Aset / Fungsi Aset	Penerimaan Risiko	Kontrol ISO 27001	Pengendalian
			A.11.2.1; Penempatan dan perlindungan alat	Semua peralatan harus ditempatkan pada tempatnya dan dilindungi untuk mengurangi risiko ancaman dan bahaya lingkungan atau memberi kesempatan akses oleh pihak yang tidak berwenang.
			A.11.2.3; Keamanan kabel	Kabel daya dan telekomunikasi (power and telecommunications cabling) yang menyalurkan data atau informasi pendukung harus dilindungi dari intersepsi, gangguan atau kerusakan.
			A.13.1.1; Kontrol jaringan (network controls)	Jaringan harus dikelola dan dikontrol untuk melindungi sistem informasi dan aplikasi.
			A.15.1.1; Kebijakan keamanan informasi untuk hubungan dengan supplier	Persyaratan keamanan informasi untuk mencegah risiko yang terkait dengan akses *supplier* terhadap aset organisasi harus disepakati dengan *supplier* dan didokumentasikan.
			A.15.2.1; Pemantauan dan pengkajian ulang jasa supplier	Organisasi harus memantau, mengkaji dan mengaudit *supplier* secara berkala.
3	Server	Risk Reduction	A.5.1.1; Kebijakan keamanan informasi	Dokumen kebijakan keamanan informasi harus disahkan oleh manajemen dan dipublikasikan serta dikomunikasikan kepada semua karyawan dan pihak-pihak lain yang relevan.
			A.6.1.1; Tugas dan tanggung jawab keamanan informasi	Semua tanggung jawab keamanan informasi harus ditetapkan dan diinformasikan.
			A.7.2.2; Kepedulian, pendidikan dan pelatihan keamanan informasi	Setiap pegawai dan kontraktor harus secara berkala mendapat pelatihan yang cukup tentang kepedulian, kebijakan dan prosedur yang berlaku sesuai dengan pekerjaan masing-masing.
			A.8.1.1; Inventarisasi aset	Aset-aset yang berhubungan dengan perangkat pemrosesan informasi harus diidentifikasi dengan jelas dan inventarisasi semua aset penting harus dicatat dan dipelihara.
			A.8.1.3; Aturan pemakaian aset	Aturan-aturan penggunaan informasi yang berhubungan dengan perangkat pemrosesan informasi harus diidentifikasi, didokumentasikan dan diterapkan.
			A.9.1.1; Kebijakan kontrol akses	Kebijakan kontrol akses harus ditetapkan, didokumentasikan dan dikaji ulang berdasarkan ketentuan bisnis dan persyaratan keamanan informasi.
			A.9.1.2; Akses ke jaringan dan layanan jaringan	*User* hanya dapat mengakses jaringan dan layanan jaringan yang telah secara spesifik diberikan kewenangan.

No	Jenis Aset / Fungsi Aset	Penerimaan Risiko	Kontrol ISO 27001	Pengendalian
			A.9.2.1; Registrasi pengguna dan pembatalan registrasi (*user registration and de-registration*)	Proses registrasi dan pembatalan *user* harus diterapkan untuk memungkinkan pemberian hak akses.
			A.9.2.2; Penyediaan user access	Proses penyediaan user access harus diimplementasikan untuk pemberian atau pembatalan hak akses terhadap semua jenis user.
			A.9.2.3; Akses ke jaringan dan layanan jaringan	User hanya dapat mengakses jaringan dan layanan jaringan yang telah secara spesifik diberikan kewenangan.
			A.9.2.5; Review terhadap hak akses user	Pemilik aset harus me-review hak akses user secara berkala.
			A.9.2.6; Penghapusan atau Penyesuaian Hak Akses	Proses penghapusan atau penutupan hak Akses untuk user yang sudah tidak berkepentingan.
			A.9.4.1; Pembatasan akses informasi	Akses terhadap informasi dan fungsi sistem aplikasi harus dibatasi sesuai dengan kebijakan kontrol akses.
			A.9.4.2; Prosedur log-on yang aman	Apabila disyaratkan kebijakan kontrol akses, akses ke sistem dan aplikasi harus dikendalikan dengan prosedur log-on.
			A.9.4.3; Sistem manajemen password	Manajemen password harus interaktif dan menjamin kualitas password.
			A.11.1.1; Perimeter keamanan fisik	Pembatas keamanan harus didefinisikan dan digunakan untuk melindungi wilayah atau ruang yang berisi informasi dan perangkat pemrosesan informasi sensitif atau kritis.
			A.11.1.2; Pengendalian akses masuk (Physical entry controls)	Area aman (secure area) harus dilindungi kontrol akses masuk yang sesuai untuk menjamin hanya orang yang berwenang yang diperbolehkan masuk.
			A.11.1.3; Keamanan kantor, ruang dan fasilitas	Keamanan fisik untuk kantor, ruang dan fasilitas harus disediakan dan diterapkan.
			A.11.1.4; Perlindungan ancaman dari luar dan lingkungan sekitar	Perlindungan fisik terhadap bencana alam, serangan berbahaya atau kecelakaan harus dibuat dan diterapkan.
			A.11.2.1; Penempatan dan perlindungan alat	Semua peralatan harus ditempatkan pada tempatnya dan dilindungi untuk mengurangi risiko ancaman dan bahaya lingkungan atau memberi kesempatan akses oleh pihak yang tidak berwenang.
			A.11.2.2; Sarana pendukung	Peralatan harus dilindungi dari power failures dan gangguan lain yang mengakitbatkan sarana pendukung tidak berfungsi.

No	Jenis Aset / Fungsi Aset	Penerimaan Risiko	Kontrol ISO 27001	Pengendalian
			A.11.2.4; Pemeliharaan peralatan	Peralatan harus dipelihara dengan benar untuk menjamin ketersediaan dan keutuhan peralatan.
			A.12.1.1; Prosedur operasi yang terdokumentasi	Prosedur pengoperasian harus didokumentasikan, dipelihara dan tersedia untuk semua user yang membutuhkan prosedur tersebut.
			A.12.3.1; Back-up informasi	Back-up copy informasi, software dan sistem gambar (system images) harus dilakukan dan diuji secara berkala sesuai dengan kebijakan back-up yang telah ditetapkan.
			A.12.4.1; Kegiatan log	Kegiatan log yang merekam aktivitas user, kelainan-kelainan, kesalahan dan kejadian keamanan informasi harus dibuat, disimpan dan di-review secara berkala.
			A.12.4.2; Perlindungan informasi log	Fasilitas log dan informasi log harus dilindungi dari gangguan dan akses secara yang tidak sah.
			A.12.4.3; Log administrator dan operator	Kegiatan sistem administrator dan operator harus direkam dan log dilindungi dan di-review secara berkala.
			A.12.5.1; Instalasi software pada sistem operasional	Prosedur harus ditetapkan untuk mengontrol instalasi software pada sistem operasional.
4	Wireless Access Point	Risk Reduction	A.5.1.1; Kebijakan keamanan informasi	Dokumen kebijakan keamanan informasi harus disahkan oleh manajemen dan dipublikasikan serta dikomunikasikan kepada semua karyawan dan pihak-pihak lain yang relevan.
			A.8.1.1; Inventarisasi aset	Aset-aset yang berhubungan dengan perangkat pemrosesan informasi harus diidentifikasi dengan jelas dan inventarisasi semua aset penting harus dicatat dan dipelihara.
			A.11.2.1; Penempatan dan perlindungan alat	Semua peralatan harus ditempatkan pada tempatnya dan dilindungi untuk mengurangi risiko ancaman dan bahaya lingkungan atau memberi kesempatan akses oleh pihak yang tidak berwenang.
			A.11.2.2; Sarana pendukung	Peralatan harus dilindungi dari power failures dan gangguan lain yang mengakitbatkan sarana pendukung tidak berfungsi.
			A.11.2.4; Pemeliharaan peralatan	Peralatan harus dipelihara dengan benar untuk menjamin ketersediaan dan keutuhan peralatan.
			A.12.1.1; Prosedur operasi yang terdokumentasi	Prosedur pengoperasian harus didokumentasikan, dipelihara dan tersedia untuk semua user yang membutuhkan prosedur tersebut.

No	Jenis Aset / Fungsi Aset	Penerimaan Risiko	Kontrol ISO 27001	Pengendalian
5	Firewall	Risk Reduction	A.5.1.1; Kebijakan keamanan informasi	Dokumen kebijakan keamanan informasi harus disahkan oleh manajemen dan dipublikasikan serta dikomunikasikan kepada semua karyawan dan pihak-pihak lain yang relevan.
			A.8.1.1; Inventarisasi aset	Aset-aset yang berhubungan dengan perangkat pemrosesan informasi harus diidentifikasi dengan jelas dan inventarisasi semua aset penting harus dicatat dan dipelihara.
			A.11.1.1; Perimeter keamanan fisik	Pembatas keamanan harus didefinisikan dan digunakan untuk melindungi wilayah atau ruang yang berisi informasi dan perangkat pemrosesan informasi sensitif atau kritis.
			A.11.1.2; Pengendalian akses masuk (Physical entry controls)	Area aman (secure area) harus dilindungi kontrol akses masuk yang sesuai untuk menjamin hanya orang yang berwenang yang diperbolehkan masuk.
			A.11.2.1; Penempatan dan perlindungan alat	Semua peralatan harus ditempatkan pada tempatnya dan dilindungi untuk mengurangi risiko ancaman dan bahaya lingkungan atau memberi kesempatan akses oleh pihak yang tidak berwenang.
			A.11.2.2; Sarana pendukung	Peralatan harus dilindungi dari power failures dan gangguan lain yang mengakitbatkan sarana pendukung tidak berfungsi.
			A.11.2.4; Pemeliharaan peralatan	Peralatan harus dipelihara dengan benar untuk menjamin ketersediaan dan keutuhan peralatan.
			A.12.1.1; Prosedur operasi yang terdokumentasi	Prosedur pengoperasian harus didokumentasikan, dipelihara dan tersedia untuk semua user yang membutuhkan prosedur tersebut.
6	Router	Risk Reduction	A.5.1.1; Kebijakan keamanan informasi	Dokumen kebijakan keamanan informasi harus disahkan oleh manajemen dan dipublikasikan serta dikomunikasikan kepada semua karyawan dan pihak-pihak lain yang relevan.
			A.8.1.1; Inventarisasi aset	Aset-aset yang berhubungan dengan perangkat pemrosesan informasi harus diidentifikasi dengan jelas dan inventarisasi semua aset penting harus dicatat dan dipelihara.
			A.11.1.1; Perimeter keamanan fisik	Pembatas keamanan harus didefinisikan dan digunakan untuk melindungi wilayah atau ruang yang berisi informasi dan perangkat pemrosesan informasi sensitif atau kritis.
			A.11.1.2; Pengendalian akses masuk (Physical entry controls)	Area aman (secure area) harus dilindungi kontrol akses masuk yang sesuai untuk menjamin hanya orang yang berwenang yang diperbolehkan masuk.

No	Jenis Aset / Fungsi Aset	Penerimaan Risiko	Kontrol ISO 27001	Pengendalian
			A.11.2.1; Penempatan dan perlindungan alat	Semua peralatan harus ditempatkan pada tempatnya dan dilindungi untuk mengurangi risiko ancaman dan bahaya lingkungan atau memberi kesempatan akses oleh pihak yang tidak berwenang.
			A.11.2.2; Sarana pendukung	Peralatan harus dilindungi dari power failures dan gangguan lain yang mengakitbatkan sarana pendukung tidak berfungsi.
			A.11.2.4; Pemeliharaan peralatan	Peralatan harus dipelihara dengan benar untuk menjamin ketersediaan dan keutuhan peralatan.
			A.12.1.1; Prosedur operasi yang terdokumentasi	Prosedur pengoperasian harus didokumentasikan, dipelihara dan tersedia untuk semua user yang membutuhkan prosedur tersebut.
7	Switch	Risk Reduction	A.5.1.1; Kebijakan keamanan informasi	Dokumen kebijakan keamanan informasi harus disahkan oleh manajemen dan dipublikasikan serta dikomunikasikan kepada semua karyawan dan pihak-pihak lain yang relevan.
			A.8.1.1; Inventarisasi aset	Aset-aset yang berhubungan dengan perangkat pemrosesan informasi harus diidentifikasi dengan jelas dan inventarisasi semua aset penting harus dicatat dan dipelihara.
			A.11.1.1; Perimeter keamanan fisik	Pembatas keamanan harus didefinisikan dan digunakan untuk melindungi wilayah atau ruang yang berisi informasi dan perangkat pemrosesan informasi sensitif atau kritis.
			A.11.1.2; Pengendalian akses masuk (Physical entry controls)	Area aman (secure area) harus dilindungi kontrol akses masuk yang sesuai untuk menjamin hanya orang yang berwenang yang diperbolehkan masuk.
			A.11.2.1; Penempatan dan perlindungan alat	Semua peralatan harus ditempatkan pada tempatnya dan dilindungi untuk mengurangi risiko ancaman dan bahaya lingkungan atau memberi kesempatan akses oleh pihak yang tidak berwenang.
			A.11.2.2; Sarana pendukung	Peralatan harus dilindungi dari power failures dan gangguan lain yang mengakitbatkan sarana pendukung tidak berfungsi.
			A.11.2.4; Pemeliharaan peralatan	Peralatan harus dipelihara dengan benar untuk menjamin ketersediaan dan keutuhan peralatan.
			A.12.1.1; Prosedur operasi yang terdokumentasi	Prosedur pengoperasian harus didokumentasikan, dipelihara dan tersedia untuk semua user yang membutuhkan prosedur tersebut.

No	Jenis Aset / Fungsi Aset	Penerimaan Risiko	Kontrol ISO 27001	Pengendalian
8	Storage Modul Disk	Risk Reduction	A.5.1.1; Kebijakan keamanan informasi	Dokumen kebijakan keamanan informasi harus disahkan oleh manajemen dan dipublikasikan serta dikomunikasikan kepada semua karyawan dan pihak-pihak lain yang relevan.
			A.8.1.1; Inventarisasi aset	Aset-aset yang berhubungan dengan perangkat pemrosesan informasi harus diidentifikasi dengan jelas dan inventarisasi semua aset penting harus dicatat dan dipelihara.
			A.11.1.1; Perimeter keamanan fisik	Pembatas keamanan harus didefinisikan dan digunakan untuk melindungi wilayah atau ruang yang berisi informasi dan perangkat pemrosesan informasi sensitif atau kritis.
			A.11.1.2; Pengendalian akses masuk (Physical entry controls)	Area aman (secure area) harus dilindungi kontrol akses masuk yang sesuai untuk menjamin hanya orang yang berwenang yang diperbolehkan masuk.
			A.11.2.1; Penempatan dan perlindungan alat	Semua peralatan harus ditempatkan pada tempatnya dan dilindungi untuk mengurangi risiko ancaman dan bahaya lingkungan atau memberi kesempatan akses oleh pihak yang tidak berwenang.
			A.11.2.2; Sarana pendukung	Peralatan harus dilindungi dari power failures dan gangguan lain yang mengakitbatkan sarana pendukung tidak berfungsi.
			A.11.2.4; Pemeliharaan peralatan	Peralatan harus dipelihara dengan benar untuk menjamin ketersediaan dan keutuhan peralatan.
			A.12.1.1; Prosedur operasi yang terdokumentasi	Prosedur pengoperasian harus didokumentasikan, dipelihara dan tersedia untuk semua user yang membutuhkan prosedur tersebut.
			A.12.3.1; Back-up informasi	Back-up copy informasi, software dan sistem gambar (system images) harus dilakukan dan diuji secara berkala sesuai dengan kebijakan back-up yang telah ditetapkan.
9	Uninterupted Power Supply (UPS)	Risk Acceptance	A.5.1.1; Kebijakan keamanan informasi	Dokumen kebijakan keamanan informasi harus disahkan oleh manajemen dan dipublikasikan serta dikomunikasikan kepada semua karyawan dan pihak-pihak lain yang relevan.
			A.8.1.1; Inventarisasi aset	Aset-aset yang berhubungan dengan perangkat pemrosesan informasi harus diidentifikasi dengan jelas dan inventarisasi semua aset penting harus dicatat dan dipelihara.
			A.11.2.1; Penempatan dan perlindungan alat	Semua peralatan harus ditempatkan pada tempatnya dan dilindungi untuk mengurangi risiko ancaman dan bahaya lingkungan atau memberi kesempatan akses oleh pihak yang tidak berwenang.

No	Jenis Aset / Fungsi Aset	Penerimaan Risiko	Kontrol ISO 27001	Pengendalian
			A.11.2.2; Sarana pendukung	Peralatan harus dilindungi dari power failures dan gangguan lain yang mengakitbatkan sarana pendukung tidak berfungsi.
			A.11.2.4; Pemeliharaan peralatan	Peralatan harus dipelihara dengan benar untuk menjamin ketersediaan dan keutuhan peralatan.
			A.12.1.1; Prosedur operasi yang terdokumentasi	Prosedur pengoperasian harus didokumentasikan, dipelihara dan tersedia untuk semua user yang membutuhkan prosedur tersebut.
10	Genset	Risk Acceptance	A.5.1.1; Kebijakan keamanan informasi	Dokumen kebijakan keamanan informasi harus disahkan oleh manajemen dan dipublikasikan serta dikomunikasikan kepada semua karyawan dan pihak-pihak lain yang relevan.
			A.8.1.1; Inventarisasi aset	Aset-aset yang berhubungan dengan perangkat pemrosesan informasi harus diidentifikasi dengan jelas dan inventarisasi semua aset penting harus dicatat dan dipelihara.
			A.11.1.1; Perimeter keamanan fisik	Pembatas keamanan harus didefinisikan dan digunakan untuk melindungi wilayah atau ruang yang berisi informasi dan perangkat pemrosesan informasi sensitif atau kritis.
			A.11.1.2; Pengendalian akses masuk (Physical entry controls)	Area aman (secure area) harus dilindungi kontrol akses masuk yang sesuai untuk menjamin hanya orang yang berwenang yang diperbolehkan masuk.
			A.11.2.1; Penempatan dan perlindungan alat	Semua peralatan harus ditempatkan pada tempatnya dan dilindungi untuk mengurangi risiko ancaman dan bahaya lingkungan atau memberi kesempatan akses oleh pihak yang tidak berwenang.
			A.11.2.2; Sarana pendukung	Peralatan harus dilindungi dari power failures dan gangguan lain yang mengakitbatkan sarana pendukung tidak berfungsi.
			A.11.2.4; Pemeliharaan peralatan	Peralatan harus dipelihara dengan benar untuk menjamin ketersediaan dan keutuhan peralatan.
			A.12.1.1; Prosedur operasi yang terdokumentasi	Prosedur pengoperasian harus didokumentasikan, dipelihara dan tersedia untuk semua user yang membutuhkan prosedur tersebut.
11	A.C. Split	Risk Reduction	A.5.1.1; Kebijakan keamanan informasi	Dokumen kebijakan keamanan informasi harus disahkan oleh manajemen dan dipublikasikan serta dikomunikasikan kepada semua karyawan dan pihak-pihak lain yang relevan.
			A.8.1.1; Inventarisasi aset	Aset-aset yang berhubungan dengan perangkat pemrosesan informasi harus diidentifikasi dengan jelas dan inventarisasi semua aset penting harus dicatat dan dipelihara.

No	Jenis Aset / Fungsi Aset	Penerimaan Risiko	Kontrol ISO 27001	Pengendalian
			A.11.2.1; Penempatan dan perlindungan alat	Semua peralatan harus ditempatkan pada tempatnya dan dilindungi untuk mengurangi risiko ancaman dan bahaya lingkungan atau memberi kesempatan akses oleh pihak yang tidak berwenang.
			A.11.2.2; Sarana pendukung	Peralatan harus dilindungi dari power failures dan gangguan lain yang mengakitbatkan sarana pendukung tidak berfungsi.
			A.11.2.4; Pemeliharaan peralatan	Peralatan harus dipelihara dengan benar untuk menjamin ketersediaan dan keutuhan peralatan.
			A.12.1.1; Prosedur operasi yang terdokumentasi	Prosedur pengoperasian harus didokumentasikan, dipelihara dan tersedia untuk semua user yang membutuhkan prosedur tersebut.
12	CCTV - Camera Control Television System	Risk Reduction	A.5.1.1; Kebijakan keamanan informasi	Dokumen kebijakan keamanan informasi harus disahkan oleh manajemen dan dipublikasikan serta dikomunikasikan kepada semua karyawan dan pihak-pihak lain yang relevan.
			A.8.1.1; Inventarisasi aset	Aset-aset yang berhubungan dengan perangkat pemrosesan informasi harus diidentifikasi dengan jelas dan inventarisasi semua aset penting harus dicatat dan dipelihara.
			A.11.2.1; Penempatan dan perlindungan alat	Semua peralatan harus ditempatkan pada tempatnya dan dilindungi untuk mengurangi risiko ancaman dan bahaya lingkungan atau memberi kesempatan akses oleh pihak yang tidak berwenang.
			A.11.2.2; Sarana pendukung	Peralatan harus dilindungi dari power failures dan gangguan lain yang mengakitbatkan sarana pendukung tidak berfungsi.
			A.11.2.4; Pemeliharaan peralatan	Peralatan harus dipelihara dengan benar untuk menjamin ketersediaan dan keutuhan peralatan.
			A.12.1.1; Prosedur operasi yang terdokumentasi	Prosedur pengoperasian harus didokumentasikan, dipelihara dan tersedia untuk semua user yang membutuhkan prosedur tersebut.
13	Alat Sidik Jari	Risk Reduction	A.5.1.1; Kebijakan keamanan informasi	Dokumen kebijakan keamanan informasi harus disahkan oleh manajemen dan dipublikasikan serta dikomunikasikan kepada semua karyawan dan pihak-pihak lain yang relevan.
			A.8.1.1; Inventarisasi aset	Aset-aset yang berhubungan dengan perangkat pemrosesan informasi harus diidentifikasi dengan jelas dan inventarisasi semua aset penting harus dicatat dan dipelihara.

No	Jenis Aset / Fungsi Aset	Penerimaan Risiko	Kontrol ISO 27001	Pengendalian
			A.11.2.1; Penempatan dan perlindungan alat	Semua peralatan harus ditempatkan pada tempatnya dan dilindungi untuk mengurangi risiko ancaman dan bahaya lingkungan atau memberi kesempatan akses oleh pihak yang tidak berwenang.
			A.11.2.2; Sarana pendukung	Peralatan harus dilindungi dari power failures dan gangguan lain yang mengakitbatkan sarana pendukung tidak berfungsi.
			A.11.2.4; Pemeliharaan peralatan	Peralatan harus dipelihara dengan benar untuk menjamin ketersediaan dan keutuhan peralatan.
			A.12.1.1; Prosedur operasi yang terdokumentasi	Prosedur pengoperasian harus didokumentasikan, dipelihara dan tersedia untuk semua user yang membutuhkan prosedur tersebut.

Tabel 4.13 Rekomendasi kebijakan berdasar kejadian ancaman keamanan informasi yang pernah terjadi di DPTSI

No.	Nama Aset	Level Risiko	Ancaman (Kejadian Yang Pernah Terjadi)	Kontrol ISO 27001	Rekomendasi
1	Sistem informasi	Medium	Database pada Sim e-Perkantoran rusak penyebab tidak diketahui	A.12.3.1; Back-up informasi	Harus dilakukan back-up seluruh database aplikasi secara periodik pada DRC dan Clouds
			Database mahasiswa baru terhapus sebelum dibackup kesalahan teknis operator	A.7.2.2; Kepedulian, pendidikan dan pelatihan keamanan informasi	Setiap pegawai di DPTSI harus memiliki kompetensi yang memadai dan melakukan perbaikan pengetahuan dengan mengikuti pelatihan yang sesuai dengan bidang kerja yang ditangani
			Data password pada database user SSO terhapus karena salah konfigurasi	A.16.1.2; Pelaporan kejadian keamanan informasi	Setiap kejadian kerusakan atau kehilangan dan perbaikan informasi dan perangkat informasi harus tercatat pada dokumen kejadian perkara.

No.	Nama Aset	Level Risiko	Ancaman (Kejadian Yang Pernah Terjadi)	Kontrol ISO 27001	Rekomendasi
			Password SSO integra yang dibagikan ke user lain	A.9.4.3; Sistem manajemen password	Pengguna yang mendapat hak akses harus melakukan penggunaan password yang kuat, yaitu kumpulan karakter yang terdiri dari huruf, angka dan simbol dengan minimal jumlah 8 karakter serta pembatasan umur password maksimal 120 hari, untuk menghindari pembobolan password oleh pihak yang tidak memiliki otoritas.
					Setiap user password yang dialihkan ke orang lain harus menggunakan surat kuasa bermaterai dengan batas maksimal penggunaan selama 30 hari, dan penerima kuasa bertanggung jawab penuh atas penggunaan user dan password tersebut.
					Pemilik user password harus melakukan penggantian password setelah masa kuasa penggunaan password kepada pihak lain berakhir.
2	Server	Medium	Kerusakan bagian (part) pada server yang berusia lebih dari 4 tahun, dimana server tersebut menjalankan aplikasi yang harus selalu mennyala dan bisa diakses	A.11.2.4; Pemeliharaan peralatan	Perangkat aset Informasi yang berusia lebih dari 4 tahun tidak boleh digunakan sebagai layanan yang bersifat kritis.
					Perangkat aset informasi yang memegang peran kritis seperti server yang sudah berusia lebih dari 4 tahun harus dipersiapkan perangkat baru sebagai penggantinya dengan spesifikasi yang lebih tinggi dan lebih canggih.
			Database mail box email ITS hilang dikarenakan HD rusak disebabkan listrik tidak stabil	A.11.2.2; Sarana pendukung	Setiap perangkat aset informasi harus mendapatkan jaminan kecukupan suplai sumber daya listrik ketika aliran listrik dari PLN padam dengan penggunaan Genset dan/atau UPS
3	Back Bone (FO) Network	Medium	Kabel Jaringan FO (Back bone) putus terkena penggalian pondasi gedung	A.11.2.3; Keamanan kabel	Setiap proses pekerjaan penggalian di lingkungan ITS harus sepengetahuan dan mendapatkan ijin dari pihak Subdirektorat Infrastruktur dan keamanan informasi DPTSI, untuk memastikan keamanan jaringan FO yang ada di ITS.

No.	Nama Aset	Level Risiko	Ancaman (Kejadian Yang Pernah Terjadi)	Kontrol ISO 27001	Rekomendasi
					Harus dibuatkan dokumen peta jaringan FO yang ada di ITS dan disosialisasikan ke unit-unit terkait di internal ITS
4	Wireless Access Point	Medium	Kesalahan konfigurasi yang berakibat jaringan tidak dapat diakses	A.7.2.2; Kepedulian, pendidikan dan pelatihan keamanan informasi	Setiap pegawai di DPTSI harus memiliki kompetensi yang memadai dan melakukan perbaikan pengetahuan dengan mengikuti pelatihan yang sesuai dengan bidang kerja yang ditangani
			Mati karena pasokan listrik PLN padam	A.11.2.2; Sarana pendukung	Setiap perangkat aset informasi harus mendapatkan jaminan kecukupan suplai sumber daya listrik ketika aliran listrik dari PLN padam dengan penggunaan Genset dan/atau UPS
			Mati karena konsleting listrik atau debu	A.11.2.4; Pemeliharaan peralatan	Pemeriksaan dan perawatan perangkat secara berkala sesuai dengan prosedur yang telah ditetapkan
			Kerusakan karena usia perangkat lebih dari 5 tahun		Perangkat aset Informasi yang berusia lebih dari 4 tahun tidak boleh digunakan sebagai layanan yang bersifat kritis.
5	Router	Medium	Kesalahan konfigurasi yang berakibat jaringan tidak dapat diakses	A.7.2.2; Kepedulian, pendidikan dan pelatihan keamanan informasi	Setiap pegawai di DPTSI harus memiliki kompetensi yang memadai dan melakukan perbaikan pengetahuan dengan mengikuti pelatihan yang sesuai dengan bidang kerja yang ditangani
			Mati karena pasokan listrik PLN padam	A.11.2.2; Sarana pendukung	Setiap perangkat aset informasi harus mendapatkan jaminan kecukupan suplai sumber daya listrik ketika aliran listrik dari PLN padam dengan penggunaan Genset dan/atau UPS
			Mati karena konsleting listrik atau debu	A.11.2.4; Pemeliharaan peralatan	Pemeriksaan dan perawatan perangkat secara berkala sesuai dengan prosedur yang telah ditetapkan
			Kerusakan karena usia perangkat lebih dari 5 tahun		Perangkat aset Informasi yang berusia lebih dari 4 tahun tidak boleh digunakan sebagai layanan yang bersifat kritis.

No.	Nama Aset	Level Risiko	Ancaman (Kejadian Yang Pernah Terjadi)	Kontrol ISO 27001	Rekomendasi
6	Switch	Medium	Kesalahan konfigurasi yang berakibat jaringan tidak dapat diakses	A.7.2.2; Kepedulian, pendidikan dan pelatihan keamanan informasi	Setiap pegawai di DPTSI harus memiliki kompetensi yang memadai dan melakukan perbaikan pengetahuan dengan mengikuti pelatihan yang sesuai dengan bidang kerja yang ditangani
			Mati karena pasokan listrik PLN padam	A.11.2.2; Sarana pendukung	Setiap perangkat aset informasi harus mendapatkan jaminan kecukupan suplai sumber daya listrik ketika aliran listrik dari PLN padam dengan penggunaan Genset dan/atau UPS
			Mati karena konsleting listrik atau debu	A.11.2.4; Pemeliharaan peralatan	Pemeriksaan dan perawatan perangkat secara berkala sesuai dengan prosedur yang telah ditetapkan
			Kerusakan karena usia perangkat lebih dari 5 tahun		Perangkat aset Informasi yang berusia lebih dari 4 tahun tidak boleh digunakan sebagai layanan yang bersifat kritis.
7	Storage Modul Disk	Medium	Database tidak dapat diakses karena kesalahan konfigurasi	A.7.2.2; Kepedulian, pendidikan dan pelatihan keamanan informasi	Setiap pegawai di DPTSI harus melakukan perbaikan pengetahuan dengan mengikuti pelatihan yang sesuai dengan bidang kerja yang ditangani
			Kerusakan karena pasokan listrik tidak stabil	A.11.2.2; Sarana pendukung	Setiap perangkat aset informasi harus mendapatkan jaminan kecukupan suplai sumber daya listrik ketika aliran listrik dari PLN padam dengan penggunaan Genset dan/atau UPS
			Kerusakan karena usia perangkat lebih dari 5 tahun	A.11.2.4; Pemeliharaan peralatan	Pemeriksaan dan perawatan perangkat secara berkala sesuai dengan prosedur yang telah ditetapkan
					Perangkat aset Informasi yang berusia lebih dari 4 tahun tidak boleh digunakan sebagai layanan yang bersifat kritis.
8	Genset	Low	Bahan bakar habis ketika genset digunakan	A.11.2.4; Pemeliharaan peralatan	Pemeriksaan dan perawatan perangkat secara berkala sesuai dengan prosedur yang telah ditetapkan
			Kabel luaran genset tidak terpasang dengan sempurna pada jalur listrik pengganti PLN, sehingga pasokan		

No.	Nama Aset	Level Risiko	Ancaman (Kejadian Yang Pernah Terjadi)	Kontrol ISO 27001	Rekomendasi
			listrik yang mengalir ke perangkat tidak stabil		
9	A.C. Split	Medium	Temperatur tidak dingin karena freon berkurang Saluran pembuangan buntu Mati karena konsleting listrik atau debu	A.11.2.4; Pemeliharaan peralatan	Pemeriksaan dan perawatan perangkat secara berkala sesuai dengan prosedur yang telah ditetapkan

[Halaman ini sengaja dikosongkan]

4.7 Penyusunan Draft Kebijakan Keamanan Informasi

Setelah kontrol ISO 27001 ditetapkan pada masing-masing aset yang telah dilakukan penilaian risikonya, maka tahapan selanjutnya yaitu penyusunan kebijakan keamanan informasi yang didasari dari langkah pengendalian keamanan sebagaimana dijelaskan pada kontrol ISO 27001.

Dalam penyusunan kebijakan keamanan informasi ini, penulis menyesuaikan sesuai dengan Panduan Penetapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Layanan Publik, yang disusun oleh Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika RI, tahun 2011. Pada buku panduan tersebut disebutkan bahwa dalam menyusun dokumen tata kelola keamanan informasi minimal harus terdiri atas 6 pokok bahasan, yaitu:

a. Kebijakan Umum Keamanan Informasi
b. Peran dan tanggung jawab organisasi keamanan informasi
c. Kebijakan Pengamanan Akses Fisik dan Lojik
d. Kebijakan Manajemen Risiko TIK
e. Manajemen Kelangsungan Usaha (Business Continuity Management)
f. Ketentuan Penggunaan Sumber Daya TIK

Selanjutnya dari kontrol ISO 27001 yang telah dipetakan pada tiap-tiap risiko aset, dikelompokkan kedalam pokok bahasan dari penyusunan kebijakan keamanan informasi tersebut diatas. Berikut tabel pemetaan kontrol ISO 27001 ke dalam pokok bahasan kebijakan keamanan informasi.

Tabel 4.14. Pemetaan kontrol ISO 27001 pada isi dokumen kebijakan keamanan

No.	Kontrol ISO 27001	Pokok Bahasan KKI
1	A.5.1.1; Kebijakan keamanan informasi	Kebijakan umum keamanan informasi
2	A.6.1.1; Tugas dan tanggung jawab keamanan informasi	Peran dan tanggung jawab organisasi keamanan informasi
3	A.6.1.3; Kontak dengan pihak berwenang	Peran dan tanggung jawab organisasi keamanan informasi
4	A.8.1.1; Inventarisasi aset	Manajemen Aset
5	A.8.1.3; Aturan pemakaian aset	Manajemen Aset
6	A.9.1.1; Kebijakan kontrol akses	Kontrol Akses
7	A.9.1.2; Akses ke jaringan dan layanan jaringan	Kontrol Akses

No.	Kontrol ISO 27001	Pokok Bahasan KKI
8	A.9.2.1; Registrasi pengguna dan pembatalan registrasi (user registration and de-registration)	Kontrol Akses
9	A.9.2.2; Penyediaan user access	Kontrol Akses
10	A.9.2.3; Akses ke jaringan dan layanan jaringan	Kontrol Akses
11	A.9.2.5; Review terhadap hak akses user	Kontrol Akses
12	A.9.2.6; Penghapusan atau Penyesuaian Hak Akses	Kontrol Akses
13	A.9.4.1; Pembatasan akses informasi	Kontrol Akses
14	A.9.4.2; Prosedur log-on yang aman	Kontrol Akses
15	A.9.4.3; Sistem manajemen password	Kontrol Akses
16	A.9.4.5; Kontrol akses terhadap program source code	Kontrol Akses
17	A.10.1.1; Kebijakan penggunaan kontrol kriptografi	Manajemen Kriptografi
18	A.11.1.1; Perimeter keamanan fisik	Pengamanan Akses Fisik dan Lingkungan
19	A.11.1.2; Pengendalian akses masuk (Physical entry controls)	Pengamanan Akses Fisik dan Lingkungan
20	A.11.1.3; Keamanan kantor, ruang dan fasilitas	Pengamanan Akses Fisik dan Lingkungan
21	A.11.1.4; Perlindungan ancaman dari luar dan lingkungan sekitar	Pengamanan Akses Fisik dan Lingkungan
22	A.11.2.1; Penempatan dan perlindungan alat	Manajemen Penggunaan Sumber Daya TIK
23	A.11.2.2; Sarana pendukung	Manajemen Penggunaan Sumber Daya TIK
24	A.11.2.3; Keamanan kabel	Manajemen Penggunaan Sumber Daya TIK
25	A.11.2.4; Pemeliharaan peralatan	Manajemen Penggunaan Sumber Daya TIK
26	A.12.1.1; Prosedur operasi yang terdokumentasi	Manajemen Komunikasi dan Operasional
27	A.12.2.1; Kontrol malware	Manajemen Komunikasi dan Operasional
28	A.12.3.1; Back-up informasi	Manajemen Komunikasi dan Operasional
29	A.12.4.1; Kegiatan log	Manajemen Komunikasi dan Operasional
30	A.12.4.2; Perlindungan informasi log	Manajemen Komunikasi dan Operasional
31	A.12.4.3; Log administrator dan operator	Manajemen Komunikasi dan Operasional
32	A.12.5.1; Instalasi software pada sistem operasional	Manajemen Komunikasi dan Operasional
33	A.13.1.1; Kontrol jaringan (network controls)	Manajemen Komunikasi dan Operasional
34	A.14.1.2; Pengamanan layanan aplikasi pada jaringan publik	Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi
35	A.14.2.1; Kebijakan pengembangan yang aman	Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi
36	A.15.1.1; Kebijakan keamanan informasi untuk hubungan dengan supplier	Hubungan dengan supplier
37	A.15.2.1; Pemantauan dan pengkajian ulang jasa supplier	Hubungan dengan supplier

No.	Kontrol ISO 27001	Pokok Bahasan KKI
38	A.16.1.2; Pelaporan kejadian keamanan informasi	Manajemen insiden keamanan informasi
39	A.16.1.3; Pelaporan kelemahan keamanan	Manajemen insiden keamanan informasi

Adapun konten dari draft kebijakan keamanan informasi tersebut disajikan pada tabel 4.15 berikut:

Tabel 4.15 Konten dari draft kebijakan keamanan informasi

NO.	Pokok Bahasan dan Konten Kebijakan
1	**Kebijakan Umum Keamanan Informasi** • Kebijakan keamanan informasi di Institut Teknologi Sepuluh Nopember menjadi panduan dan pedoman untuk melaksanakan kegiatan yang ada hubungannya dengan keamanan informasi di Institut ini. • Kebijakan keamanan informasi harus disosialisasikan dan dikomunikasikan ke seluruh Dosen, Pegawai, Mahasiswa dan pihak ketiga terkait melalui media komunikasi yang ada agar dipahami dengan mudah dan dipatuhi. • Seluruh kelemahan keamanan informasi yang berpotensi atau telah mengakibatkan gangguan penggunaan TI harus segera dilaporkan ke penanggung jawab TI terkait. • Setiap pelanggaran terhadap kebijakan ini yang relevan dapat dikenai sanksi atau tindakan disiplin sesuai peraturan yang berlaku. • Setiap detail teknis pelaksanaan tata kelola keamanan informasi yang tidak tercantum dalam kebijakan keamanan ini diatur dengan prosedur dan petunjuk pelaksanaan. • Perubahan atau penambahan pada kebijakan informasi harus disetujui oleh bagian yang berkaitan, dan bisa dipertanggungjawabkan.
2	**Peran dan Tanggung Jawab Organisasi Keamanan Informasi** • Rektor mendelegasikan sebagian tanggung jawab Tata Kelola TI di Institut Teknologi Sepuluh Nopember kepada DPTSI yang ditetapkan melalui Surat Keputusan Rektor no.10 Tahun 2016, tentang Organisasi dan Tata Kerja ITS. • DPTSI bertanggung jawab untuk memberikan rekomendasi strategis kepada Rektor atas hasil Evaluasi, Arahan dan Pengawasan Teknologi Informasi di ITS. • Peran Organisasi Keamanan Informasi di Institut Teknologi Sepuluh Nopember adalah: a. Mencegah terjadinya kehilangan atau kerusakan informasi di ITS b. Mengurangi risiko dari ancaman dari luar yang berkaitan dengan informasi di ITS. c. Menjaga informasi yang ada tidak digunakan secara sembarangan oleh pihak yang tidak d. Berwenang. • Struktur organisasi keamanan informasi dibentuk atas dasar kepentingan realisasi Peran Strategis keamanan informasi di ITS. • Rektor menetapkan Kebijakan Keamanan Informasi Institut melalui Surat Keputusan Rektor, dan melaksanakan peninjauna ulang secara berkala agar kebijakan sesuai dengan situasi dan kondisi terkini.

3	**Manajemen Aset** • Seluruh aset yang berkaitan dengan keamanan informasi harus tercatat dalam SIM e-Aset, diberi label penanda dan diawasi pada jangka waktu yang ditentukan, baik aset fisik maupun non fisik. • Setiap Seksi di DPTSI harus melakukan analisa resiko setiap asset sesuai dengan prosedur yang tertulis di Pedoman Instruksi Kerja. • Setiap perubahan dokumen daftar asset dan analisa resiko harus di tandatangani oleh kepala seksi , kasubdit dan Direktur. • DPTSI harus membuat pedoman tentang klasifikasi keamanan informasi, tata keloka informasi, penghancuran informasi. • Setiap pemindahan aset fisik harus dilengkapi dengan berita acara perpindahan aset yang ditandatangi oleh kepala seksi dan kasubdit. • Setiap Seksi harus membuat prosedur pemakaian aset dan tata cara perawatan aset. • Peralatan sumber daya informasi institut harus ditempatkan dengan aman dan terlindung untuk menurunkan risiko terhadap ancaman lingkungan dan bahaya serta peluang dari akses yang tidak memiliki wewenang, serta terlindungi dari kegagalan suplai sumber daya energi dan gangguan lainnya yang diakibatkan kegagalan utility pendukung. • Penggunaan peralatan sumber daya informasi institut di luar area kerja lingkungan institut harus mendapatkan persetujuan pihak atasan atau manajemen yang terkait dan tercatat. • Setiap kerusakan aset harus dilaporkan kepada petugas Aset dan dicatat dalam berita acara kerusakan aset. • Setiap kejadian kehilangan dan perbaikan informasi dan perangkat informasi harus tercatat pada dokumen kejadian perkara. • Penggantian aset karena kerusakan haruslah dengan spesifikasi aset yang sesuai atau lebih tinggi dari aset yang rusak. • Perangkat aset Informasi yang berusia lebih dari 4 tahun tidak boleh digunakan sebagai layanan yang bersifat kritis. • Penghapusan aset dilakukan sesuai dengan aturan pemerintah dan dipastikan tidak ada informasi yang masih tersimpan didalamnya.
4.	**Kontrol Akses** • Setiap pengguna yang akan mengakses seluruh sistem informasi dan layanan informasi lainnya harus terdaftar dan mendapat izin akses dari unit kerja DPTSI dan atau unit kerja pemilik informasi. • Hak akses akan diberikan kepada pengguna dalam bentuk user-id yang unik serta password yang kuat oleh unit kerja Teknologi dan Keamanan informasi dan atau unit kerja pemilik informasi. • Pengguna yang mendapat hak akses harus melakukan penggunaan password yang kuat, yaitu kumpulan karakter yang terdiri dari huruf, angka dan symbol dengan minimal jumlah 8 karakter serta pembatasan umur password maksimal 120 hari, untuk menghindari pembobolan password oleh pihak yang tidak memiliki otoritas. • Setiap pengguna jaringan harus terdaftar dan mendapat izin akses dari DPTSI. • Unit kerja DPTSI harus melakukan pengendalian koneksi pada layanan jaringan melalui: a. Pemisahan jaringan harus berdasarkan grup layanan informasi, kelompok pengguna atau unit kerja serta lokasi dengan menerapkan segmentasi jaringan. b. Harus dilakukan pembatasan jumlah akses dan waktu akses terhadap layanan jaringan yang di-share c. Pengendalian harus di setiap jalur jaringan terhadap setiap koneksi komputer dan alur informasi, sehingga tidak terjadi pelanggaran hak akses terhadap aplikasi bisnis

	• Pembatasan akses informasi dan fungsi-fungsi harus terdapat pada sistem aplikasi, merupakan wewenang dan tanggung jawab DPTSI. • Setiap user password yang dialihkan ke orang lain harus menggunakan surat kuasa bermaterai dengan batas maksimal penggunaan selama 30 hari, dan penerima kuasa bertanggung jawab penuh atas penggunaan user dan password tersebut. • Pemilik user password harus melakukan penggantian password setelah masa kuasa penggunaan password kepada pihak lain berakhir. • DPTSI harus membuat prosedur pengamanan log-on pada sistem operasi dan Database • Pengamanan log-on pada sistem operasi harus diberikan kepada pengguna dalam bentuk user-id yang unik dan digunakan secara personal serta menggunakan password yang kuat sebagai teknik otentifikasi yang memadai dan terkelola secara interaktif. • Ketentuan lebih lanjut tentang hak akses diatur dalam pedoman instruksi kerja tata kelola hak akses, dan instruksi kerja manajemen password untuk Administrator.
5	**Manajemen Kriptografi**
	• Semua sistem yang dikelola dan/atau dikembangkan oleh DPTSI, harus menerapkan enkripsi pada hak akses (user dan password) yang dikelola. • Proses enkripsi dapat dilakukan pada sistem database atau level aplikasi. • Teknologi enkripsi yang digunakan harus mengikuti perkembangan teknologi kriptografi.
6	**Pengamanan Akses Fisik dan Lingkungan**
	• DPTSI harus melakukan klasifikasi area kerja di institut dengan membuat table klasifikasi area kerja yaitu : VIP/terlarang, Terbatas dan Umum. • Area terlarang/VIP seperti data-center dan area terbatas harus memiliki pengamanan fisik ganda, seperti pintu akses bergembok atau pengaman sidik jari. • Area terlarang/VIP harus menggunakan pengamanan fisik yang dapat tahan terhadap kerusakan yang diakibatkan oleh api, banjir, gempa bumi, ledakan, kerusuhan masa dan bentuk lain dari bencana yang disebabkan oleh alam atau oleh perbuatan manusia. • Setiap personil yang akan masuk ke area kerja harus memiliki identitas diri dan tercatat pada satuan pengamanan. • Pihak ketiga hanya diperbolehkan masuk ke area terlarang/VIP umtuk tujuan khusus perawatan dan perbaikan yang tidak mampu dilakukan sendiri oleh DPTSI dan dalam pengawasan ketat. • Seluruh lingkungan kantor dan lokasi aset informasi kritis harus terpasang kamera perekam CCTV yang aktif 24 jam dan data rekaman bisa diakses selama 30 hari terakhir. • Setiap aset atau perangkat perbaikan yang akan akan masuk dan keluar dari area terlarang/VIP harus diperiksa dan diverifikasi oleh petugas DPTSI • Dilarang membawa perangkat komunikasi dan media perekam apapun ketika memasuki area terlarang/VIP. • Setiap proses pekerjaan penggalian di lingkungan ITS harus sepengetahuan dan mendapatkan ijin dari pihak Subdirektorat Infrastruktur dan keamanan informasi DPTSI, untuk memastikan keamanan jaringan FO yang ada di ITS. • Peta jaringan FO yang ada di ITS harus terdokumentasi dan disosialisasikan ke unit-unit terkait di internal ITS.
7	**Manajemen Penggunaan Sumber Daya TIK**
	• Setiap perangkat aset informasi yang digunakan harus ditempatkan pada lokasi yang aman, dan terlindung dari gangguan luar namun mudah untuk di akses. • Setiap perangkat aset informasi harus mendapatkan jamiman kecukupan suplai sumber daya listrik ketika aliran listrik dari PLN padam.

	• Setiap pemasangan kabel jaringan baik jaringan *Fiber Optic* ataupun jaringan LAN harus mendapatkan jaminan keamanan dari gangguan yang dapat menyebabkan kerusakan fisik atau hilangnya informasi yang ditrsnmisikan. • Semua perangkat keras aset informasi harus dilakukan perawatan secara berkala sesuai dengan prosedure perawatan aset yang telah ditetapkan.
8	**Manajemen Komunikasi dan Operasional**
	• Setiap seksi di DPTSI harus memiliki pedoman prosedur dan instruksi kerja untuk setiap pekerjaan. • Setiap ada perubahan atau penambahan infrastruktur jaringan atau konfigurasi jaringan seksi network harus melakukan uji coba terlebih dahulu, dan ujicoba harus sepengetahuan Direktur dan Kepala Subdirektorat Infrastruktur dan Keamanan Teknologi Informasi. • Subdirektorat Infrastruktur dan Keamanan Teknologi Informasi harus memiliki capacity manajement plan tentang storage, infrastruktur, dan bandwidth. • Setiap ada perubahan atau penambahan pada database dan aplikasi yang dikelola oleh DPTSI harus melakukan ujicoba terlebih dahulu, dan ujicoba harus sepengetahuan Direktur dan Kepala Subdirektorat Pengembangan Sistem Informasi. • Setiap ujicoba yang dilakukan harus direncanakan dan didokumentasikan. • Untuk melakukan proteksi terhadap malware dan virus pada personal computer dilingkungan ITS, DPTSI mewajibkan untuk mengunakan penggunaan sistem operasi dan aplikasi berlisensi yang terupdate. Serta melarang menggunakan perangkat lunak ilegal dalam bentuk apapun. • Untuk melakukan proteksi terhadap malware pada server , DPTSI menggunakan firewall dengan proteksi terkini. • Untuk back up dan recovery diatur sesuai dengan prosedur Backup dan recovery • Untuk melindungi sumber daya informasi dari bencana, baik yang disebabkan oleh alam atau oleh manusia, seksi infrastruktur dan keamanan informasi harus melakukan back-up dengan membuat Disaster Recovery Center (DRC). • Untuk pengelolaan dan monitoring log pada network dan network services merupakan tanggungjawab seksi infrastruktur dan keamanan informasi, sedangkan log database dan aplikasi merupakan tanggungjawab seksi pengembangan SI. • Untuk manajemen log dikelola dengan software yang telah ditentukan oleh seksi infrastruktur. • Log yang tersimpan hanya boleh diakses oleh administrator sistem • Hasil pencatatan (file log) harus di back-up, dianalisa dan dilakukan tindakan lanjutan yang sesuai. • Seksi infrastruktur dan keamanan informasi harus melakukan pengelolaan dan pengendalian jaringan dengan melakukan identifikasi setiap informasi dan sumber daya informasi yang terhubung jaringan kampus, baik jaringan yang dikelola sendiri ataupun pihak ketiga.
9	**Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi**
	• Setiap pembuatan aplikasi, baik itu baru atau penambahan modul maka harus ada tahap testing • Proses berbagi (*sharing*) data, seperti data pengajian pegawai dan dosen dan data mahasiswa pembayaran biaya pendidikan mahasiswa dengan pihak bank, dilakukan atas dasar kerjasama dan dilengkapi dengan dokumen kerjasama dan keamanan yang sangat baik dan terukur. • Setiap pengembangan dan pemeliharaan sistem harus tetap memenuhi aspek kerahasiaan, keutuhan, ketersediaan, dan otentikasi serta otorisasi pada sistem informasi.
10	**Hubungan dengan supplier**
	• Proses Pengadaan barang dan jasa di DPTSI mengacu pada peraturan perundang-undangan yang berlaku. • Proses pemilihan supplier untuk pengadaan barang dan jasa di DPTSI mengacu pada peraturan perundang-undangan yang berlaku. • Subdirektorat Infrastruktur dan Keamanan Teknologi Informasi melakukan analisis penilaian resiko supplier barang dan jasa di DPTSI ITS. • Pengelolaan perubahan jasa supplier diatur sesuai dengan peraturan perundang undangan yang berlaku.

11	**Manajemen insiden keamanan informasi**
	• Unit kerja DPTSI harus membuat prosedur mekanisme pelaporan dan penanganan terhadap kejadian keamanan informasi. • Unit kerja DPTSI harus melakukan dokumentasi terhadap seluruh pelaporan kejadian keamanan informasi, baik yang disampaikan secara lisan maupun tertulis, baik dalam bentuk dokumen ataupun dalam bentuk elektronik (email, form elektronik dan sebagainya). • Kegiatan sosialisasi, awareness dan pelatihan harus dilaksanakan kepada seluruh stakeholder ITS terhadap sistem informasi dan layanan untuk berperan serta memberikan laporan terhadap hasil pengamatan atau kecurigaan terhadap kelemahan keamanan pada sistem dan layanan di ITS. • Unit kerja DPTSI harus melakukan dokumentasi terhadap seluruh kegiatan penanganan kecelakaan keamanan informasi, berdasarkan hasil tindakan perbaikan pelaksanaan, baik dari pihak internal maupun eksternal.
12	**Manajemen Kontinyuitas Bisnis**
	• DPTSI harus membuat Disaster Recovery Plan (DRP) sebagai pemenuhan Business Continuity Management (BCM) aspek keamanan informasi. • DPTSI harus membuat Disaster Recovery Center (DRC) sebagai tindak lanjut dokumen Disaster Recovery Plan (DRP).
13	**Kepatuhan Terhadap Ketentuan yang Berlaku**
	• DPTSI melakukan pemeriksaan terhadap pemenuhan teknis standar keamanan pada sistem informasi secara berkala. Pemeriksaan pemenuhan teknis standar keamanan harus terdokumentasi, terpelihara dan dilakukan tinjauan ulang secara berkala untuk memastikan tetap up to date dengan kebutuhan bisnis dan perkembangan teknologi serta efektif terhadap penerapan dan pelaksanaan pemenuhan standar yang ada di ITS. • DPTSI harus melakukan audit atas keefektifan penerapan dan pelaksanaan keamanan informasi dan ketidaksesuaian terhadap kebijakan keamanan, standar keamanan dan pemenuhan teknis serta hukum, undang-undang, regulasi atau kewajiban kontrak terkait keamanan informasi yang berlaku di ITS. • DPTSI melakukan dokumentasi terhadap kegiatan dan hasil audit yang dilakukan untuk dilakukan tinjauan ulang oleh Rektor sebagai tindak lanjut perbaikan terhadap ketidaksesuaian di ITS. • Semua pihak yang bermaksud untuk melakukan tindakan pengrusakan, mencurian dan atau penyalahgunaan informasi yang ada di lingkungan ITS ada dikenakan sanksi senagaimana undanng-undang yang berlaku.

4.8 Verifikasi dan Validasi Draft Dokumen Kebijakan Keamanan Informasi

Setelah draf dokumen kebijakan keamanan informasi tersusun selanjutnya dilakukan lakukan tahap verivikasi dan validasi oleh pihak DPTSI, khususnya Subdirektorat Infrastruktur dan Keamanan Teknologi Informasi, Subdirektorat Pengembangan Sistem Informasi dan Subdirektorat Layanan Teknologi dan Sistem Informasi.

Verifikasi dan validasi tersebut disesuai dengan tingkat kebutuhan keamanan informasi di ITS dan disetujui oleh seluruh kasubdit dan direktur DPTSI.

Tabel 4.16 Verifikasi kesesuaian draft kebijakan keamanan informasi dengan kebutuhan ITS.

No.	Pokok Bahasan KKI	Kesesuaian Kebutuhan
1	Kebijakan umum keamanan informasi	V
2	Peran dan tanggung jawab organisasi keamanan informasi	V
3	Manajemen Aset	V
4	Kontrol Akses	V
5	Manajemen Kriptografi	V
6	Pengamanan Akses Fisik dan Lingkungan	V
7	Manajemen Penggunaan Sumber Daya TIK	V
8	Manajemen Komunikasi dan Operasional	V
9	Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi	V
10	Hubungan dengan supplier	V
11	Manajemen insiden keamanan informasi	V
12	Manajemen Kontinyuitas Bisnis	V
13	Kepatuhan Terhadap Ketentuan yang Berlaku	V

BAB 5
KESIMPULAN DAN SARAN

Bab ini menjelaskan kesimpulan dan saran yang diperoleh berdasarkan keseluruhan proses yang dilakukan selama penelitian berlangsung untuk meyakinkan bahwa hasil penelitian yang didapatkan menjawab rumusan dan tujuan dari penelitian.

5.1 Kesimpulan

Berdasarkan hasil penelitian yang dilakukan maka ada beberapa hal yang dapat disimpulkan sebagaimana berikut:

1. Dari 1212 aset BMN yang dikelola oleh DPTSI ITS, terdapat 670 aset informasi yang mana 215 termasuk aset kritis dan selanjutnya dikelompokkan menjadi 61 kelompok aset kritis berdasarkan kesamaan jenis aset, merek dan type, fungsi serta tahun perolehan.
2. Penilaian risiko terhadap 61 kelompok aset kritis yang dikelola oleh DPTSI ITS didapatkan hasil sebagai berikut:
   - 10 kelompok aset kritis yang memiliki level risiko *LOW*.
   - 51 kelompok Aset yang level risikonya *MEDIUM*.
3. Penerima risiko terhadap 10 kelompok aset yang memiliki level risiko *LOW* adalah *Risk Acceptance*, sedangkan untuk 51 kelompok aset yang memiliki level risiko *MEDIUM* penerimaan risiko yang dipilih yaitu *Risk Reduction* dengan melaksukan kontrol keamanan berdasar kontrol ISO 27001:2013.
4. Berdasar kejadian ancaman keamanan informasi yang pernah terjadi pada DPTSI ITS, maka domain kontrol ISO 27001:2013 yang masuk **prioritas** dalam penyusunan kebijakan keamanan di lingkungan kampus ITS, yaitu:
   - A.5.1.1; Kebijakan keamanan informasi
   - A.7.2.2; Kepedulian, pendidikan dan pelatihan keamanan informasi
   - A.9.4.3; Sistem manajemen password
   - A.11.2.1; Penempatan dan perlindungan alat
   - A.11.2.2; Sarana pendukung

- A.11.2.3; Keamanan kabel
- A.11.2.4; Pemeliharaan peralatan
- A.12.1.1; Prosedur operasi yang terdokumentasi
- A.12.3.1; Back-up informasi
- A.16.1.2; Pelaporan kejadian keamanan informasi

5.2 Saran

Adapun saran yang dapat diberikan dari hasil penelitian terhadap risiko keamanan informasi ini yaitu:

1. Perlu dilakukan penelitian dengan metode penilaian yang berbeda dalam mengukur risiko keamanan informasi yang ada di ITS, hal ini dapat dijadikan sebagai pembanding hasil penelitian yang telah dilakukan apakah memang penilaian risiko tersebut telah sesuai.
2. Dalam penyusunan kebijakan keamanan informasi tersebut hendaknya dilengkapi dengan penelitian tindak kesadaran (*awareness*) terhadap keamanan informasi pada seluruh anggota organisasi IT.

DAFTAR PUSTAKA

Andress, J., Leary, M.R., 2016. Building a Practical Information Security Program. Elsevier Science, s.l.

Cheung, S.K.S., 2014. Information Security Management for Higher Education Institutions, in: Pan, J.-S., Snasel, V., Corchado, E.S., Abraham, A., Wang, S.-L. (Eds.), Intelligent Data Analysis and Its Applications, Volume I. Springer International Publishing, Cham, pp. 11–19. https://doi.org/10.1007/978-3-319-07776-5_2

Deloitte Australia, Shedden, P., Ahmad, A., University of Melbourne, Smith, W., University of Melbourne, Tscherning, H., Deakin University, Scheepers, R., Deakin University, 2016. Asset Identification in Information Security Risk Assessment: A Business Practice Approach. Commun. Assoc. Inf. Syst. 39, 297–320. https://doi.org/10.17705/1CAIS.03915

Dey, M., 2007. Information security management-a practical approach, in: AFRICON 2007. IEEE, pp. 1–6.

Doherty, N.F., Fulford, H., 2006. Aligning the information security policy with the strategic information systems plan. Comput. Secur. 25, 55–63. https://doi.org/10.1016/j.cose.2005.09.009

EC-Council, 2010. Network Defense: Security Policy and Threats. Cengage Learning.

Eloff, J.H., Eloff, M., 2003. Information security management: a new paradigm, in: Proceedings of the 2003 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on Enablement through Technology. South African Institute for Computer Scientists and Information Technologists, pp. 130–136.

Etsebeth, V., 2006. Information Security Policies-The Legal Risk of Uninformed Personnel., in: ISSA. pp. 1–10.

Flowerday, S.V., Tuyikeze, T., 2016. Information security policy development and implementation: The what, how and who. Comput. Secur. 61, 169–183. https://doi.org/10.1016/j.cose.2016.06.002

Ghazvini, A., Shukur, Z., Hood, Z., 2018. Review of information security policy based on content coverage and online presentation in higher education. Int. J. Adv. Comput. Sci. Appl. 9, 410–423.

Höne, K., Eloff, J.H.P., 2002. Information security policy—what do international information security standards say? Comput. Secur. 21, 402–409.

Hong, K.-S., Chi, Y.-P., Chao, L.R., Tang, J.-H., 2003. An integrated system theory of information security management. Inf. Manag. Comput. Secur. 11, 243–248.

ISO/IEC 27000:2016(E), 2016.

Kadam, A.W., 2007. Information Security Policy Development and Implementation. Inf. Syst. Secur. 16, 246–256. https://doi.org/10.1080/10658980701744861

Kementerian Keuangan, 2016. PERATURAN MENTERI KEUANGAN REPUBLIK INDONESIA, NOMOR 181 /PMK.06/2016 TENTANG PENATAUSAHAAN BARANG MILIK NEGARA.

Kementerian Keuangan, 2013. KEPUTUSAN MENTERI KEUANGAN NOMOR: 59/KMK.6/2013 TENTANG TABEL MASA MANFAAT DALAM RANGKA PENYUSUTAN BARANG MILIK NEGARA BERUPA ASET TETAP PADA ENTITAS PEMERINTAH PUSAT.

Knapp, K.J., Franklin Morris, R., Marshall, T.E., Byrd, T.A., 2009. Information security policy: An organizational-level process model. Comput. Secur. 28, 493–508. https://doi.org/10.1016/j.cose.2009.07.001

Laudon, K.C., Traver, C.G., 2016. E-commerce 2016: Business, Technology, Society, 12th Edition. ed. Pearson College Div.

Maynard, S., Ruighaver, A.B., 2002. Evaluating IS Security Policy Development, in: 3rd Australian Information Warfare and Security Conference.

McIlwraith, A., 1993. Security policies—A security officer's perspective. Comput. Audit Update 1993, 10–14.

Mirela, G., Maria, B.D., 2008. Information Security Management System. ANALELE Univ. DIN ORADEA 1353.

Moody, D.L., Walsh, P., 1999. Measuring the Value Of Information-An Asset Valuation Approach., in: ECIS. pp. 496–512.

Ølnes, J., 1994. Development of security policies. Comput. Secur. 13, 628–636.

Peltier, T.R., 2002. Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. Auerbach Publications, Boca Raton, Fla.

Posthumus, S., von Solms, R., 2004. A framework for the governance of information security. Comput. Secur. 23, 638–646. https://doi.org/10.1016/j.cose.2004.10.006

Raggad, B.G., 2010. Information Security Management : Concepts and Practice. CRC Press, Boca Raton.

Rahmad, B., Supangkat, S.H., Sembiring, J., Surendro, K., 2010. Threat Scenario Dependency-Based Model of Information Security Risk Analysis. IJCSNS 10, 93.

Rencana Strategi ITS tahun 2014-2018, 2014. . Institut Teknologi Sepuluh Nopember, Surabaya.

Sari, P.K., Nurshabrina, N., 2016. Factor analysis on information security management in higher education institutions, in: 2016 4th International Conference on Cyber and IT Service Management. IEEE, pp. 1–5.

Sarno, R., Iffano, I., 2009. Sistem Manajemen Keamanan Informasi Berbasis ISO 27001. ITSPress.

Soto, M., 2011. The Enterprise Information Security Policy as a Strategic Business Policy within the Corporate Strategic Plan.

Stair, R.M., Reynolds, G.W., 2010. Fundamentals of information systems. Course Technology, Boston.

Symantec's 2017 Internet Security Threat Report (ISTR), 2017. , Volume 22. Symantec.

Tittel, E., 2002. Understanding Security Policies.

Torres, J.M., Sarriegi, J.M., Santos, J., Serrano, N., 2006. Managing information systems security: critical success factors and indicators to measure effectiveness, in: International Conference on Information Security. Springer, pp. 530–545.

Tuyikeze, T., Pottas, D., 2011. An Information Security Policy Development Life Cycle, in: Proceedings of the South African Information Security Multi-Conference: Port Elizabeth, South Africa, 17-18 May 2010. Lulu. com, p. 165.

Ulmer, J., Bandyopadhyay, S., Spafford, E., 2003. PFIRES: A policy framework for information security. Commun ACM 46, 101–106. https://doi.org/10.1145/792704.792706

Von Solms, B., Von Solms, R., 2004. The 10 deadly sins of information security management. Comput. Secur. 23, 371–376. https://doi.org/10.1016/j.cose.2004.05.002

Von Solms, S.H., 1997. Selection of secure single sign-on solutions for heterogeneous computing environments, in: Information Security in Research and Business. Springer, pp. 9–24.

Wahsheh, L.A., Alves-Foss, J., 2008. Security policy development: Towards a life-cycle and logic-based verification model. Am. J. Appl. Sci. 5, 1117–1126.

Whitman, M.E., Mattord, H.J., 2014. Management of information security, Fourth edition. ed. Cengage Learning, Stamford, CT, USA.

Whitman, M.E., Mattord, H.J., 2012. Principles of information security, 4th ed. ed. Course Technology, Boston, MA.

Yustanti, W., Qoiriah, A., Bisma, R., Prihanto, A., 2018. An analysis of Indonesia's information security index: a case study in a public university. IOP Conf. Ser. Mater. Sci. Eng. 296, 012038. https://doi.org/10.1088/1757-899X/296/1/012038

[Halaman ini sengaja dikosongkan]

LAMPIRAN

Lampiran A

Daftar Kontrol Keamanan Informasi ISO/IEC 27001:2013

A.5 Kebijakan keamanan informasi		
A 5.1 Arahan manajemen untuk keamanan informasi Sasaran: Memberikan arahan manajemen organisasi dan dukungan keamanan informasi dalam hubungan dengan persyaratan bisnis organisasi dan peraturan perundang-undangan yang berlaku.		
A. 5.1.1	Kebijakan keamanan informasi	Pengendalian: Dokumen kebijakan keamanan informasi harus disahkan oleh manajemen dan dipublikasikan serta dikomunikasikan kepada semua karyawan dan pihak-pihak lain yang relevan.
A.5.1.2	Kaji ulang kebijakan keamanan informasi	Pengendalian: Kebijakan keamanan informasi harus dikaji ulang secara berkala, atau jika terjadi perubahan untuk memastikan kecukupan dan keefektifan kebijakan informasi yang berkelanjutan.
A.6 Organisasi keamanan informasi		
A.6.1 Organisasi internal Sasaran: Membentuk kerangka kerja manajemen untuk memulai dan mengendalikan pelaksanaan operasi keamanan informasi dalam organisasi.		
A.6.1.1	Tugas dan tanggung jawab keamanan informasi	Pengendalian: Semua tanggung jawab keamanan informasi harus ditetapkan dan diinformasikan.
A.6.1.2	Pemisahan tugas	Pengendalian: Tugas yang saling bertentangan harus dipisahkan untuk mengurangi peluang perubahan yang tidak sah atau tidak disengaja atau penyalahgunaan aset organisasi.
A.6.1.3	Kontak dengan pihak berwenang	Pengendalian: Kontak dengan pihak berwenang yang relevan harus dipelihara.
A.6.1.4	Kontak dengan kelompok khusus (*special interest groups*)	Pengendalian: Kontak dengan kelompok khusus atau forum ahli keamanan informasi dan asosiasi profesi harus dipelihara.
A.6.1.5	Keamanan informasi dalam *project management*	Pengendalian: Keamanan informasi harus dibahas dalam *project management* terlepas dari jenis proyek.

A.6.2 Perangkat *mobile* dan *teleworking*		
Sasaran: Untuk menjamin keamanan *teleworking* dan penggunaan perangkat *mobile*.		
A.6.2.1	Kebijakan perangkat mobile	Pengendalian: Kebijakan dan langkah-langkah keamanan harus diterapkan untuk mengelola risiko akibat penggunaan perangkat mobile.
A.6.2.2	*Teleworking*	Pengendalian: Kebijakan dan langkah-langkah keamanan harus diterapkan untuk melindungi informasi yang diakses, diproses atau disimpan di lokasi *teleworking*.
A.7 Keamanan Sumber Daya Manusia (SDM)		
A.7.1 Sebelum bekerja		
Sasaran: Untuk memastikan karyawan dan kontraktor memahami akan tanggung jawabnya sesuai dengan perannya.		
A.7.1.1	Seleksi (*screening*)	Pengendalian: Pemeriksaan latar belakang calon karyawan dan kontraktor harus dilaksanakan sesuai dengan peraturan perundang-undangan yang berlaku, etika yang berlaku dan proporsional terhadap persyaratan bisnis, klasifikasi informasi yang akan diakses dan risiko yang mungkin dihadapi organisasi.
A.7.1.2	Persyaratan dan ketentuan kepegawaian	Pengendalian: Calon pegawai dan kontraktor harus menyetujui dan menandatangani syarat dan aturan kontrak kepegawaian yang menyatakan tanggung jawab keamanan informasi.
A.7.2 Selama bekerja		
Sasaran: Untuk memastikan karyawan dan kontraktor memahami dan memenuhi tanggung jawab keamanan informasi.		
A.7.2.1	Tanggung jawab manajemen	Pengendalian: Manajemen harus mewajibkan setiap pegawai dan kontraktor menerapkan keamanan informasi sesuai dengan kebijakan dan prosedur yang berlaku.
A.7.2.2	Kepedulian, pendidikan dan pelatihan keamanan informasi	Pengendalian: Setiap pegawai dan kontraktor harus secara berkala mendapat pelatihan yang cukup tentang kepedulian, kebijakan dan prosedur yang berlaku sesuai dengan pekerjaan masing-masing.

A.7.2.3	Kedisiplinan	Pengendalian: Proses kedisiplinan secara formal harus diberlakukan dan dikomunikasikan ke seluruh pegawai yang melakukan pelanggaran keamanan informasi.
A.7.3 Pemberhentian karyawan dan pemindahan pekerjaan Sasaran: Untuk melindungi kepentingan organisasi sebagai bagian dari proses pemindahan atau pemberhentian pegawai.		
A.7.3.1	Tanggung jawab pemindahan atau pemberhentian pekerjaan	Pengendalian: Tugas dan tanggung jawab terhadap keamanan informasi harus ditetapkan untuk pemindahan atau pemberhentian pegawai dan dikomunikasikan kepada pegawai atau kontraktor.
A.8 Manajemen asset		
A.8.1 Tanggung jawab terhadap asset Sasaran: Untuk mengidentifikasi aset organisasi dan menetapkan tanggung jawab yang sesuai.		
A.8.1.1	Inventarisasi aset	Pengendalian: Aset-aset yang berhubungan dengan perangkat pemrosesan informasi harus diidentifikasi dengan jelas dan inventarisasi semua aset penting harus dicatat dan dipelihara.
A 8.1.2	Kepemilikan aset	Pengendalian: Aset investarisasi harus ada pemilik.
A. 8.1.3	Aturan pemakaian aset	Pengendalian: Aturan-aturan penggunaan informasi yang berhubungan dengan perangkat pemrosesan informasi harus diidentifikasi, didokumentasikan dan diterapkan.
A.8.1.4	Pengambilan aset	Pengendalian: Semua pegawai dan pihak luar harus mengembalikan semua aset yang digunakannya saat mereka dinyatakan berhenti bekerja sesuai dengan perjanjian kontrak.
A.8.2 Klasifikasi informasi Sasaran: Untuk menjamin setiap informasi dalam organisasi mendapatkan keamanan yang memadai berdasarkan tingkat kepentingan organisasi.		
A.8.2.1	Klasifikasi informasi	Pengendalian: Informasi harus diklasifikasi menurut nilai, peraturan hukum, sensitivitas dan tingkat kepentingabhhn (kritikal).

A.8.2.2	Pelabelan informasi	Pengendalian: Prosedur harus dibuat untuk pelabelan informasi sesuai dengan klasifikasi informasi yang telah ditentukan oleh organisasi.
A.8.2.3	Penanganan informasi	Pengendalian: Prosedur penanganan informasi harus dibuat sesuai dengan klasifikasi informasi yang telah ditentukan organisasi.
A.8.3 Penanganan media Sasaran: untuk mencegah pengaksesan, perubahan, pemindahan atau penghapusan informasi yang tersimpan dalam media.		
A.8.3.1	Manajemen *removable media*	Pengendalian: Prosedur harus diterapkan untuk mengelola *removable media* sesuai dengan klasifikasi yang ditetapkan organisasi.
A.8.3.2	Pemusnahan media	Pengendalian: Media harus dimusnahkan secara aman jika tak lagi digunakan dengan mengacu prosedur yang berlaku.
A.8.3.3	Transfer media fisik	Pengendalian: Media yang berisikan informasi harus dilindungi dari akses yang tidak sah, penggunaan ilegal atau kerusakan selama transportasi.
A.9 Kontrol akses		
A.9.1 Persyaratan bisnis untuk kontrol akses Sasaran: Untuk membatasi akses informasi dan akses ke perangkat pemrosesan informasi.		
A.9.1.1	Kebijakan kontrol akses	Pengendalian: Kebijakan kontrol akses harus ditetapkan, didokumentasikan dan dikaji ulang berdasarkan ketentuan bisnis dan persyaratan keamanan informasi.
A.9.1.2	Akses ke jaringan dan layanan jaringan	Pengendalian: *User* hanya dapat mengakses jaringan dan layanan jaringan yang telah secara spesifik diberikan kewenangan.
A.9.2 Manajemen akses user (*User access management*) Sasaran: untuk menjamin akses pengguna yang sah dan untuk mencegah pihak yang tidak sah pada sistem dan layanan.		

A.9.2.1	Registrasi pengguna dan pembatalan registrasi (*user registration and de-registration*)	Pengendalian: Proses registrasi dan pembatalan *user* harus diterapkan untuk memungkinkan pemberian hak akses.
A.9.2.2	Penyediaan *user access*	Pengendalian: Proses penyediaan *user access* harus diimplementasikan untuk pemberian atau pembatalan hak akses terhadap semua jenis *user*.
A.9.2.3	Manajemen hak akses khusus/istimewa	Pengendalian: Alokasi dan penggunaan hak akses khusus harus dibatasi dan dikendalikan.
A.9.2.4	Pengelolaan kerahasiaan otentikasi informasi (*authentication information*) *user*	Pengendalian: Alokasi atas kerahasiaan otentikasi harus dikendalikan melalui proses manajemen formal.
A.9.2.5	*Review* terhadap hak akses *user*	Pengendalian: Pemilik aset harus me-*review* hak akses *user* secara berkala.
A.9.2.6	Penghapusan atau Penyesuaian Hak Akses	Pengendalian: Proses penghapusan atau penutupan hak Akses untuk user yang sudah tidak berkepentingan.
A.9.3 Tanggung jawab *user* Sasaran: Sebagai jaminan *user* bertanggung jawab menjaga informasi otentikasi (*authentication information)*.		
A.9.3.1	Penggunaan kerahasiaan informasi otentikasi (*authentication information*)	Pengendalian: *User* wajib mengikuti praktek-praktek organisasi dalam penggunakan kerahasiaan informasi otentikasi.
A.9.4 Kontrol akses sistem dan aplikasi Sasaran: Untuk mencegah akses tidak sah ke dalam sistem dan aplikasi.		
A.9.4.1	Pembatasan akses informasi	Pengendalian: Akses terhadap informasi dan fungsi sistem aplikasi harus dibatasi sesuai dengan kebijakan kontrol akses.
A.9.4.2	Prosedur *log-on* yang aman	Pengendalian: Apabila disyaratkan kebijakan kontrol akses, akses ke sistem dan aplikasi harus dikendalikan dengan prosedur *log-on*.
A.9.4.3	Sistem manajemen *password*	Pengedalian: Manajemen *password* harus interaktif dan menjamin kualitas *password*.

A.9.4.4	Penggunaan program *utility* khusus	Pengendalian: Penggunaan program *utility* yang kemungkinan mampu menolak (*overriding*) sistem dan aplikasi harus dibatasi dan dikontrol secara ketat.
A.9.4.5	Kontrol akses terhadap program *source code*	Pengendalian: Akses ke program *source code* harus dibatasi.
A.10 Kriptografi (*Cryptography*)		
A.10.1 Kontrol kriptografi Sasaran: Untuk memastikan penggunaan kriptografi yang tepat dan efektif dalam melindungi kerahasiaan, keaslian atau integritas informasi		
A.10.1.1	Kebijakan penggunaan kontrol kriptografi	Pengendalian: Kebijakan penggunaan kontrol kriptografi untuk memproteksi informasi harus dikembangkan dan diimplementasikan.
A.10.1.2	Manajemen kunci (*key management*)	Pengendalian: Kebijakan tentang penggunaan, perlindungan dan *lifetime* kunci kriptografi harus dikembangkan dan dilaksanakan.
A.11 Keamanan fisik dan lingkungan		
A.11.1 Area yang aman Sasaran: Untuk mencegah akses yang tidak sah, kerusakan dan gangguan terhadap informasi dan perangkat pemrosesan informasi		
A.11.1.1	Perimeter keamanan fisik	Pengendalian: Pembatas keamanan harus didefinisikan dan digunakan untuk melindungi wilayah atau ruang yang berisi informasi dan perangkat pemrosesan informasi sensitif atau kritis.
A.11.1.2	Pengendalian akses masuk (*Physical entry controls*)	Pengendalian: Area aman (*secure area*) harus dilindungi kontrol akses masuk yang sesuai untuk menjamin hanya orang yang berwenang yang diperbolehkan masuk.
A.11.1.3	Keamanan kantor, ruang dan fasilitas	Pengendalian: Keamanan fisik untuk kantor, ruang dan fasilitas harus disediakan dan diterapkan.
A.11.1.4	Perlindungan ancaman dari luar dan lingkungan sekitar	Pengendalian: Perlindungan fisik terhadap bencana alam, serangan berbahaya atau kecelakaan harus dibuat dan diterapkan.

A.11.1.5	Bekerja di area aman (*Working in secure areas*)	Pengendalian: Prosedur bekerja di daerah aman harus dibuat dan diterapkan.
A.11.1.6	Area pengiriman dan bongkar muat	Pengendalian: Area-area seperti area bongkar muat dan area keluar-masuk orang harus dikontrol dan, jika mungkin, dipisahkan dari fasilitas pemrosesan informasi untuk menghindari akses informasi oleh pihak yang tidak berwenang.
A.11.2 Peralatan Sasaran: Untuk mencegah kehilangan, kerusakan, pencurian atau gangguan aset dan gangguan kegiatan terhadap operasional organisasi.		
A.11.2.1	Penempatan dan perlindungan alat	Pengendalian: Semua peralatan harus ditempatkan pada tempatnya dan dilindungi untuk mengurangi risiko ancaman dan bahaya lingkungan atau memberi kesempatan akses oleh pihak yang tidak berwenang.
A.11.2.2	Sarana pendukung	Pengendalian: Peralatan harus dilindungi dari *power failures* dan gangguan lain yang mengakitbatkan sarana pendukung tidak berfungsi.
A.11.2.3	Keamanan kabel	Pengendalian: Kabel daya dan telekomunikasi (*power and telecommunications cabling*) yang menyalurkan data atau informasi pendukung harus dilindungi dari intersepsi, gangguan atau kerusakan.
A.11.2.4	Pemeliharaan peralatan	Pengendalian: Peralatan harus dipelihara dengan benar untuk menjamin ketersediaan dan keutuhan peralatan.
A.11.2.5	Pemindahan aset	Pengendalian: Peralatan, informasi atau *software* tidak boleh dibawa keluar lokasi tanpa ijin pihak yang berwenang.
A.11.2.6	Keamanan peralatan dan aset di luar lokasi	Pengendalian: Keamanan harus diterapkan terhadap aset yang berada diluar lokasi organisasi dengan mempertimbangkan risiko saat bekerja di luar lokasi organisasi.

A.11.2.7	Kemananan pembuangan peralatan atau penggunaan kembali	Pengendalian: Peralatan yang digunakan sebagai media penyimpanan harus diverifikasi dengan benar untuk menjamin bahwa setiap data sensitif termasuk *software* berlisensi telah dihapus atau ditimpa (*overwritten*) secara aman sebelum dibuang.
A.11.2.8	Peralatan yang ditinggal oleh *user* (*unattended user equipment*)	Pengendalian: *User* harus menjamin bahwa peralatan tanpa pengawasan (*unattended*) telah dilindungi secara memadai.
A.11.2.9	C*lear desk* dan *clear screen*	Pengendalian: Kebijakan *clear desk* untuk kertas dan media penyimpanan bergerak/berpindah (*removable*) dan kebijakan *clear screen* untuk fasilitas pemrosesan informasi harus dijalankan.
A.12 Keamanan operasi		
A.12.1 Prosedur operasional dan tanggung jawab Sasaran: Untuk memastikan operasi fasilitas pemrosesan informasi dilakukan secara benar dan aman.		
A.12.1.1	Prosedur operasi yang terdokumentasi	Pengendalian: Prosedur pengoperasian harus didokumentasikan, dipelihara dan tersedia untuk semua *user* yang membutuhkan prosedur tersebut.
A.12.1.2	Manajemen perubahan	Pengendalian: Perubahan organisasi, proses bisnis, fasilitas pengolahan informasi dan sistem yang mempengaruhi keamanan informasi harus dikendalikan.
A.12.1.3	Manajemen kapasitas	Pengendalian: Penggunaan sumber daya harus dimonitor, disesuaikan dan direncanakan untuk kebutuhan masa depan (kapasitas dan persyaratan) guna menjaga performa sistem.
A.12.1.4	Pemisahan fasilitas pengembangan, pengujian dan lingkungan operasional	Pengendalian: Fasilitas pengembangan, pengujian dan operasional harus dipisahkan untuk mengurangi risiko akses atau perubahan yang tidak sah atau perubahan lingkungan operasional.
A.12.2 Perlindungan terhadap *malware* Sasaran: Untuk memastikan informasi dan fasilitas pengolahan informasi dilindungi terhadap *malware*.		

A.12.2.1	Kontrol *malware*	Pengendalian: Kontrol yang bersifat pendeteksian, pencegahan dan pemulihan agar terlindung dari *malware* untuk memberikan kesadaran *user* harus diterapkan.
A.12.3 *Back-up* Sasaran: Untuk melindungi terhadap kehilangan data.		
A.12.3.1	*Back-up* informasi	Pengendalian: *Back-up copy* informasi, *software* dan sistem gambar (*system images*) harus dilakukan dan diuji secara berkala sesuai dengan kebijakan *back-up* yang telah ditetapkan.
A.12.4 Log dan Pemantauan (*logging and monitoring*) Sasaran: Untuk merekam peristiwa dan penyediaan bukti.		
A.12.4.1	Kegiatan log	Pengendalian: Kegiatan log yang merekam aktivitas *user*, kelainan-kelainan, kesalahan dan kejadian keamanan informasi harus dibuat, disimpan dan di-*review* secara berkala.
A.12.4.2	Perlindungan informasi log	Pengendalian: Fasilitas log dan informasi log harus dilindungi dari gangguan dan akses secara yang tidak sah.
A.12.4.3	Log administrator dan operator	Pengendalian: Kegiatan sistem administrator dan operator harus direkam dan log dilindungi dan di-*review* secara berkala.
A.12.4.4	Sinkronisasi waktu	Pengendalian: Penunjuk waktu dari seluruh sistem pemrosesan informasi dalam organisasi atau domain keamanan harus disinkronisasikan dengan satu sumber penunjuk waktu.
A.12.5 Kontrol operasional *software* Sasaran: Untuk memastikan integritas sistem operasional.		
A.12.5.1	Instalasi *software* pada sistem operasional	Pengendalian: Prosedur harus ditetapkan untuk mengontrol instalasi *software* pada sistem operasional.
A.12.6 Manajemen teknik kelemahan (*vulnerability*) Sasaran: Untuk mencegah eksploitasi kelemahan teknis.		

A.12.6.1	Kontrol terhadap kelemahan secara teknis (*vulnerability*)	Pengendalian: Informasi yang tepat waktu tentang kelemahan teknis dari sistem informasi yang digunakan harus ditemukan, dievaluasi, dan diukur secara tepat untuk diketahui risiko yang terkait.
A.12.6.2	Pembatasan instalasi *software*	Pengendalian: Peraturan instalasi *software* harus diterapkan dan dijalankan.
A.12.7 Audit sistem informasi Sasaran: Untuk mengurangi dampak dari kegiatan audit pada sistem operasional.		
A.12.7.1	Kontrol audit sistem informasi	Pengendalian: Persyaratan audit dan kegiatan yang melibatkan pemeriksaan pada sistem operasional harus direncanakan secara hati-hati dan disetujui untuk mengurangi risiko dari gangguan terhadap proses bisnis.
A.13 Keamanan komunikasi		
A.13.1 Manajemen keamanan jaringan (*Network security management*) Sasaran: Untuk menjamin perlindungan informasi dalam jaringan dan mendukung fasilitas pengolahan informasinya.		
A.13.1.1	Kontrol jaringan (*network controls*)	Pengendalian: Jaringan harus dikelola dan dikontrol untuk melindungi sistem informasi dan aplikasi.
A.13.1.2	Keamanan layanan jaringan	Pengendalian: Fitur keamanan, tingkat pelayanan dan persyaratan manajemen untuk semua layanan jaringan harus diidentifikasi dan tercakup dalam perjanjian layanan jaringan, baik layanan disediakan secara *in-house* atau di-subkontraktorkan.
A.13.1.3	Pemisahan jaringan (*segregation in networks*)	Pengendalian: Grup layanan informasi, pengguna dan sistem informasi harus dipisahkan dalam jaringan.
A.13.2 Transfer informasi Sasaran: Untuk menjaga keamanan transfer informasi dalam organisasi dan pihak eksternal.		
A.13.2.1	Kebijakan dan prosedur transfer informasi	Pengendalian: Kebijakan, prosedur dan aturan transfer informasi harus ditetapkan guna melindungi pertukaran informasi melalui

		penggunaan segala tipe fasilitas komunikasi.
A.13.2.2	Perjanjian pertukaran (*exchange agreements*)	Pengendalian: Perjanjian yang memuat pertukaran informasi harus ditetapkan antara organisasi dengan pihak eksternal.
A.13.2.3	Pesan elektronik (*electronic messaging*)	Pengendalian: Informasi dalam bentuk pesan elektronik harus dilindungi dengan tepat.
A.13.2.4	Perjanjian kerahasiaan dan perjanjian *non-disclosure*	Pengendalian: Perjanjian kerahasiaan atau perjanjian *non-disclosure* yang dibutuhkan organisasi untuk melindungi informasi harus diidentifikasi dan dikaji secara regular.
A.14 Sistem akuisisi, pengembangan dan pemeliharaan		
A.14.1 Persyaratan keamanan sistem informasi Sasaran: untuk memastikan bahwa keamanan informasi merupakan bagian dari sistem informasi di seluruh siklus hidup. Hal ini juga mencakup persyaratan untuk sistem informasi yang menyediakan layanan melalui jaringan publik.		
A.14.1.1	Analisis dan spesifikasi persyaratan keamanan informasi	Pengendalian: Persyaratan keamanan informasi harus dimasukkan dalam persyaratan untuk sistem informasi baru atau perangkat tambahan untuk sistem informasi yang ada.
A.14.1.2	Pengamanan layanan aplikasi pada jaringan publik	Pengendalian: Informasi yang melewati jaringan publik harus dilindungi dari aktivitas penipuan, perselisihan kontrak, pengungkapan yang tidak sah dan modifikasi.
A.14.1.3	Perlindungan transaksi layanan aplikasi	Pengendalian: Informasi yang terlibat dalam transaksi layanan aplikasi harus dilindungi untuk mencegah *incomplete transmission*, *mis-routing*, perubahan pesan yang tidak sah, pengungkapan yang tidak sah, duplikasi pesan yang tidak sah atau *replay*.
A.14.2 Keamanan dalam proses pengembangan dan proses-proses pendukung Sasaran: Untuk memastikan bahwa keamanan informasi dibuat dan dilaksanakan dalam siklus pengembangan sistem informasi.		
A.14.2.1	Kebijakan pengembangan yang aman	Pengendalian: Aturan pengembangan *software* dan sistem harus ditetapkan dan diterapkan

		untuk proses pengembangan dalam organisasi.
A.14.2.2	Prosedur perubahan kontrol	Pengendalian: Perubahan implementasi harus dikontrol dengan menggunakan prosedur kontrol perubahan
A.14.2.3	*Review* teknis aplikasi setelah perubahan sistem operasi	Pengendalian: Jika sistem operasi berubah, aplikasi bisnis yang kritis harus ditinjau dan diuji untuk menjamin tidak berdampak pada operasional atau keamanan organisasi.
A.14.2.4	Pembatasan perubahan paket *software*	Pengendalian: Modifikasi paket *software* harus dihindari, dibatasi hanya pada perubahan yang perlu, dan seluruh perubahan harus dikontrol secara ketat.
A.14.2.5	Prinsip *system engineering* yang aman	Pengendalian: Prinsip-prinsip untuk keamanan *system engineering* harus ditetapkan, didokumentasikan, dipelihara dan diterapkan pada setiap upaya implementasi sistem informasi.
A.14.2.6	Proses pengembangan yang aman	Pengendalian: Organisasi harus menetapkan dan melindungi proses *system development* dan upaya integrasi yang mencakup seluruh siklus *system development*.
A.14.2.7	*Outsourced development*	Pengendalian: Organisasi harus memonitor kegiatan pengembangan sistem *outsourcing*.
A.14.2.8	Testing keamanan sistem	Pengendalian: Testing fungsi keamanan harus dilakukan selama proses pengembangan.
A.14.2.9	Testing *system acceptance*	Pengendalian: Program testing dan *system acceptance* harus ditetapkan untuk sistem informasi baru, upgrade dan versi baru.
A.14.3 Tes data Sasaran: Untuk melindungi data yang digunakan untuk kegiatan testing.		
A.14.3.1	Perlindungan tes data	Pengendalian: Tes data harus dipilih secara hati-hati, dan dilindungi serta dikontrol.

A.15 Hubungan dengan *supplier*		
A.15.1 Keamanan informasi dalam hubungan dengan *supplier* Sasaran: Untuk memastikan perlindungan aset organisasi yang dapat diakses oleh *supplier*.		
A.15.1.1	Kebijakan keamanan informasi untuk hubungan dengan *supplier*	Pengendalian:
A.15.1.2	Mematuhi keamanan informasi dalam perjanjian *supplier*	Pengendalian: Semua persyaratan keamanan informasi yang relevan harus ditetapkan dan disetujui oleh setiap *supplier* yang dapat mengakses, memproses, menyimpan, berkomunikasi, atau menyediakan komponen infrastruktur IT milik organisasi.
A.15.1.3	Teknologi informasi dan komunikasi *supply chain*	Pengendalian: Perjanjian dengan *supplier* harus mencakup persyaratan untuk mencegah risiko keamanan informasi yang terkait dengan teknologi informasi dan komunikasi layanan termasuk *supply chain* produk.
A.15.2 Manajemen layanan *supplier* Sasaran: untuk menerapkan dan menjaga tingkat keamanan informasi dalam hal layanan jasa yang sesuai dengan perjanjian layanan jasa dari *supplier*.		
A.15.2.1	Pemantauan dan pengkajian ulang jasa *supplier*	Pengendalian: Organisasi harus memantau, mengkaji dan mengaudit *supplier* secara berkala.
A.15.2.2	Mengelola perubahan layanan *supplier*	Pengendalian: Perubahan layanan *supplier* termasuk layanan pemeliharaan dan peningkatan kebijakan, prosedur dan pengendalian keamanan informasi yang ada, harus dikelola dengan mempertimbangkan tingkat kritikal sistem dan proses bisnis terkait dan asesmen ulang dari risiko.
A.16 Manajemen insiden keamanan informasi		
A.16.1 Manajemen insiden keamanan informasi dan perbaikan Sasaran: Untuk memastikan pendekatan yang konsisten dan efektif terhadap pengelolaan insiden keamanan informasi, termasuk komunikasi pada kejadian keamanan informasi (*security events*).		
A.16.1.1	Tanggung jawab dan prosedur	Pengendalian: Tanggung jawab manajemen dan prosedur-prosedur harus dibuat untuk memastikan tanggapan yang cepat, efektif

		dan teratur dalam mengatasi insiden keamanan informasi.
A.16.1.2	Pelaporan kejadian keamanan informasi	Pengendalian: Kejadian keamanan informasi harus dilaporkan kepada manajemen yang tepat secepat mungkin.
A.16.1.3	Pelaporan kelemahan keamanan	Pengendalian: Semua karyawan dan kontraktor yang menggunakan sistem informasi milik organisasi diwajibkan mencatat dan melaporkan setiap kelemahan keamanan yang diamati atau dicurigai dalam sistem atau layanan.
A.16.1.4	Asesmen dan keputusan tentang kejadian keamanan informasi	Pengendalian: Kejadian keamanan informasi harus diases dan diambil keputusan jika kejadian ini diklasifikasikan sebagai insiden keamanan informasi atau tidak.
A.16.1.5	Respon terhadap insiden keamanan informasi	Pengendalian: Insiden keamanan informasi harus ditanggapi sesuai dengan prosedur terdokumentasi.
A.16.1.6	Belajar dari insiden keamanan informasi	Pengendalian: Pengetahuan yang diperoleh dari menganalisis dan menyelesaikan insiden keamanan informasi harus digunakan untuk mengurangi kemungkinan atau dampak kejadian di masa depan.
A.16.1.7	Pengumpulan bukti (*Collection of evidence*)	Pengendalian: Organisasi harus menetapkan dan menerapkan prosedur untuk identifikasi, pengumpulan, akuisisi dan pemeliharaan informasi, yang dapat berfungsi sebagai bukti.
A.17 *Business Continuity Management* (BCM)		
A.17.1 Keamanan informasi dalam *Business Continuity Management* Sasaran: Kesinambungan keamanan informasi harus terintegrasi dalam sistem manajemen kelangsungan bisnis organisasi.		
A.17.1.1	Perencanaan keamanan informasi yang berkesinambungan	Pengendalian: Organisasi harus menetapkan persyaratan untuk keamanan informasi dan kesinambungan manajemen keamanan informasi dalam situasi yang merugikan, misalnya selama krisis atau bencana.
A.17.1.2	Menerapkan keamanan informasi yang berkesinambungan	Pengendalian:

		Organisasi harus menetapkan, mendokumentasikan, menerapkan dan memelihara proses, prosedur dan kontrol guna memastikan tingkat yang diperlukan keamanan informasi yang berkesinambungan selama situasi yang merugikan.
A.17.1.3	Verifikasi, *review* dan evaluasi keamanan informasi yang berkesinambungan	Pengendalian: Organisasi harus melakukan verifikasi terhadap aktifitas pengendalian keamanan informasi yang berkesinambungan secara berkala untuk memastikan bahwa pengendalian ini valid dan efektif dalam situasi yang merugikan.
A.17.2 *Redundancies* Sasaran: Untuk memastikan ketersediaan fasilitas pengolahan informasi.		
A.17.2.1	Ketersediaan fasilitas pengolahan informasi	Pengendalian: Fasilitas pengolahan informasi harus dilakukan dengan *redundancies* yang cukup untuk memenuhi kebutuhan ketersediaan.
A.18 Kesesuaian (*compliance*)		
A.18.1 Kepatuhan terhadap persyaratan hukum dan kontrak Sasaran: untuk mencegah pelanggaran hukum, peraturan perundang-undangan, peraturan atau kewajiban kontrak dan setiap persyaratan keamanan informasi.		
A.18.1.1	Identifikasi peraturan hukum yang berlaku dan persyaratan kontrak	Pengendalian: Seluruh peraturan perundang-undangan dan persyaratan kontrak serta cara organisasi untuk memenuhi persyaratan tersebut harus ditetapkan secara eksplisit, dikomunikasikan dan selalu up-date untuk tiap-tiap sistem informasi dan organisasi.
A.18.1.2	Hak kekayaan intelektual (HAKI)	Pengendalian: Prosedur yang sesuai harus diterapkan untuk memastikan kesesuaian dengan peraturan hukum, peraturan perundang-undangan dan perjanjian kontrak dalam penggunaan material yang memiliki HAKI dan penggunaan *software* yang legal.
A.18.1.3	Perlindungan rekaman organisasi	Pengendalian: Rekaman penting harus dilindungi dari kehilangan, penghancuran, pemalsuan, akses tidak sah dan rilis tidak sah sesuai dengan peraturan perundang-undangan, persyaratan kontrak dan bisnis.

A.18.1.4	Perlindungan data dan rahasia informasi pribadi	Pengendalian: Perlindungan data dan rahasia informasi pribadi harus dijamin sesuai dengan undang-undang dan peraturan yang berlaku.
A.18.1.5	Regulasi pengendalian kriptografi	Pengendalian: Pengendalian kriptografi harus sesuai dengan perjanjian yang telah disepakati, peraturan perundang-undangan dan regulasi yang berlaku.
A.18.2 *Review* keamanan informasi Sasaran: Untuk memastikan keamanan informasi diimplementasikan dan dioperasikan sesuai dengan kebijakan dan prosedur organisasi.		
A.18.2.1	Kajian ulang secara independen terhadap keamanan informasi	Pengendalian: Pendekatan organisasi dalam mengelola dan menerapkan keamanan informasi (misalnya sasaran pengendalian, kontrol, kebijakan, proses, dan prosedur kemananan informasi) harus dikaji ulang secara berkala dan independen, atau ketika terjadi perubahan signifikan terhadap penerapan keamanan.
A.18.2.2	Pemenuhan kebijakan keamanan dan standar	Pengendalian: Manajer harus memastikan bahwa seluruh prosedur keamanan dalam area tanggung jawabnya dilakukan dengan benar untuk mencapai pemenuhan kebijakan keamanan dan standar yang ditetapkan.
A.18.2.3	*Review* pemenuhan teknis	Pengendalian: Sistem informasi harus dinilai secara berkala terhadap kebijakan dan standar keamanan informasi organisasi.

Lampiran B

Data Aset DPTSI yang daiambil dari SIM E-Aset ITS

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
1	3010304003	Stationary Generating Set	1		9/18/2006	LL / R Genset Blkang Perpustakaan	Rusak	Aset Non TI
2	3020102003	Mini Bus	1	ISUZU PANTHER	11/20/2006	/ Kendaraan Operasional	Baik	Aset Non TI
3	3020104001	Sepeda Motor	1	Honda Supra Fit	11/24/2006	/ Kendaraan Operasional	Baik	Aset Non TI
4	3030307010	Scanner (Universal Tester)	1	Canon DR 3060	1/1/2003	B03-2 / R. Proses Data	Baik	Aset TI
5	3030307010	Scanner (Universal Tester)	2	Canon DR 9080C	1/1/2003	B03-2 / R. Proses Data	Baik	Aset TI
6	3050101008	Mesin Ketik Elektronik/Selektrik	2	Brother	12/12/2012	B02 / R Adm	Rusak	Aset Non TI
7	3050102003	Mesin Hitung Elektronik/Calculator	1	Karce/KC-519	12/16/2016	B02 / R Adm	Baik	Aset Non TI
8	3050102003	Mesin Hitung Elektronik/Calculator	2	Casio/MJ-120P	12/16/2016	B02 / R Adm	Baik	Aset Non TI
9	3050102003	Mesin Hitung Elektronik/Calculator	3	Casio/DX-1205-B	12/16/2016	B02-4 / R Direktur	Baik	Aset Non TI
10	3050102007	Mesin Penghitung Uang	1	Newmark	8/11/2017	B02 / R Adm	Baik	Aset Non TI
11	3050103007	Mesin Fotocopy Folio	2	IR 2520	11/10/2010	B02 / R Adm	Baik	Aset Non TI
12	3050104001	Lemari Besi/Metal	1	Yamanaka	11/11/2002	A05-3 /	Baik	Aset Non TI
13	3050104001	Lemari Besi/Metal	2	VIP 2 pintu	11/11/2002	B01-3 /	Baik	Aset Non TI
14	3050104001	Lemari Besi/Metal	3	Lemari Besi bostinco	11/11/2002	A05 /	Baik	Aset Non TI
15	3050104001	Lemari Besi/Metal	4	Asahi	11/11/2002	/	Baik	Aset Non TI
16	3050104001	Lemari Besi/Metal	5	bostinco	11/11/2002	A08 /	Baik	Aset Non TI
17	3050104001	Lemari Besi/Metal	6	VIP, 2 pintu	11/11/2002	B01-3 /	Baik	Aset Non TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
18	3050104001	Lemari Besi/Metal	7	bostinco	11/11/2002	/	Baik	Aset Non TI
19	3050104001	Lemari Besi/Metal	8	Bostinco	11/11/2002	A10 /	Baik	Aset Non TI
20	3050104001	Lemari Besi/Metal	9	Bostinco	11/11/2002	/	Baik	Aset Non TI
21	3050104001	Lemari Besi/Metal	10	Bostinco	11/11/2002	/	Baik	Aset Non TI
22	3050104001	Lemari Besi/Metal	11	Bostinco	11/11/2002	/	Baik	Aset Non TI
23	3050104001	Lemari Besi/Metal	12	VIP 2 pintu	11/11/2002	B01-3 /	Baik	Aset Non TI
24	3050104001	Lemari Besi/Metal	13	Bostinco	11/11/2002	/	Baik	Aset Non TI
25	3050104001	Lemari Besi/Metal	14	VIP, 2 pintu	11/11/2002	B01-3 /	Baik	Aset Non TI
26	3050104001	Lemari Besi/Metal	15	Bostinco	11/11/2002	/	Baik	Aset Non TI
27	3050104001	Lemari Besi/Metal	16	Lemari kaca/piring Besi	11/11/2002	A08 / R Dapur	Baik	Aset Non TI
28	3050104001	Lemari Besi/Metal	18	Cabling rack	12/17/2012	A06 / R ME	Baik	Aset Non TI
29	3050104002	Lemari Kayu	1	Blockteak	11/11/2002	A10 / Gd ATK	Baik	Aset Non TI
30	3050104002	Lemari Kayu	2	Win Exel	9/22/2008	A05 / R Layanan TSI	Baik	Aset Non TI
31	3050104003	Rak Besi	1		9/30/2015	A03 / Musholla	Baik	Aset Non TI
32	3050104003	Rak Besi	2		9/30/2015	AA00 / Selasar Utara	Baik	Aset Non TI
33	3050104003	Rak Besi	3		9/30/2015	AA00 / Selasar Utara	Baik	Aset Non TI
34	3050104003	Rak Besi	4		9/30/2015	B02 / R Keu & Adm	Baik	Aset Non TI
35	3050104003	Rak Besi	5		9/30/2015	B02 / R Keu & Adm	Baik	Aset Non TI
36	3050104003	Rak Besi	6		9/30/2015	B02 / R Keu & Adm	Baik	Aset Non TI
37	3050104003	Rak Besi	7		9/30/2015	B02-4 /	Baik	Aset Non TI
38	3050104003	Rak Besi	8	Rak Besi	11/11/2002	/	Baik	Aset Non TI
39	3050104003	Rak Besi	9	Abacus Dinding	11/11/2002	/	Baik	Aset Non TI
40	3050104003	Rak Besi	10	Abacus Dinding	11/11/2002	/	Baik	Aset Non TI
41	3050104003	Rak Besi	11	Rak Besi	11/11/2002	/	Baik	Aset Non TI
42	3050104003	Rak Besi	12	Rak Besi tanpa merk	11/11/2002	/	Baik	Aset Non TI
43	3050104003	Rak Besi	13	Rak Besi	11/11/2002	A10 /	Baik	Aset Non TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
44	3050104003	Rak Besi	14	Rak besi Double Coloumn	11/11/2002	A04 /	Baik	Aset Non TI
45	3050104003	Rak Besi	15	Rak besi	11/11/2002	A10 /	Baik	Aset Non TI
46	3050104003	Rak Besi	16	Abacus Dinding	11/11/2002	/	Baik	Aset Non TI
47	3050104003	Rak Besi	17	Rak Besi	11/11/2002	A10 /	Baik	Aset Non TI
48	3050104003	Rak Besi	18	Rak besi Single Coloumn	11/11/2002	A04 /	Baik	Aset Non TI
49	3050104003	Rak Besi	19	Rak besi	11/11/2002	A10 /	Baik	Aset Non TI
50	3050104003	Rak Besi	20	Abacus	11/11/2002	/	Baik	Aset Non TI
51	3050104003	Rak Besi	21	Abacus Dinding	11/11/2002	/	Baik	Aset Non TI
52	3050104003	Rak Besi	22	Rak besi	11/11/2002	/	Baik	Aset Non TI
53	3050104003	Rak Besi	23	Rak besi Double Coloumn	11/11/2002	/	Baik	Aset Non TI
54	3050104003	Rak Besi	24	Abacus Dinding	11/11/2002	/	Baik	Aset Non TI
55	3050104003	Rak Besi	25	Abacus Dinding	11/11/2002	/	Baik	Aset Non TI
56	3050104003	Rak Besi	26	Abacus Dinding	11/11/2002	/	Baik	Aset Non TI
57	3050104003	Rak Besi	27	Abacus Dinding	11/11/2002	/	Baik	Aset Non TI
58	3050104003	Rak Besi	28	Rak Besi	11/11/2002	/	Baik	Aset Non TI
59	3050104003	Rak Besi	29	Rak Besi	11/11/2002	/	Baik	Aset Non TI
60	3050104003	Rak Besi	30	Rak besi	11/11/2002	/	Baik	Aset Non TI
61	3050104003	Rak Besi	31	Abacus pintu kaca	11/11/2002	/	Baik	Aset Non TI
62	3050104003	Rak Besi	32	Rak Besi	11/11/2002	/	Baik	Aset Non TI
63	3050104003	Rak Besi	33	Rak besi	11/11/2002	/	Baik	Aset Non TI
64	3050104003	Rak Besi	34	Abacus Dinding	11/11/2002	/	Baik	Aset Non TI
65	3050104003	Rak Besi	35	Rak besi	11/11/2002	/	Baik	Aset Non TI
66	3050104003	Rak Besi	36	Rak Besi tanpa merk	11/11/2002	/	Baik	Aset Non TI
67	3050104003	Rak Besi	37	Rak Besi	11/11/2002	/	Baik	Aset Non TI
68	3050104003	Rak Besi	38	Rak besi	11/11/2002	/	Baik	Aset Non TI
69	3050104003	Rak Besi	39	Abacus	11/11/2002	/	Baik	Aset Non TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
70	3050104003	Rak Besi	40	Rak besi Double Coloumn	11/11/2002	/	Baik	Aset Non TI
71	3050104003	Rak Besi	41	Rak besi	11/11/2002	/	Baik	Aset Non TI
72	3050104003	Rak Besi	42	Rak Besi	11/11/2002	/	Baik	Aset Non TI
73	3050104003	Rak Besi	43	Rak besi	11/11/2002	/	Baik	Aset Non TI
74	3050104003	Rak Besi	44	Rak besi	11/11/2002	/	Baik	Aset Non TI
75	3050104003	Rak Besi	45	Abacus pintu kaca	11/11/2002	/	Baik	Aset Non TI
76	3050104003	Rak Besi	46	Abacus	11/11/2002	/	Baik	Aset Non TI
77	3050104003	Rak Besi	47	Rak besi	11/11/2002	/	Baik	Aset Non TI
78	3050104003	Rak Besi	48	Rak Besi	11/11/2002	/	Baik	Aset Non TI
79	3050104003	Rak Besi	49	Rak besi	11/11/2002	/	Baik	Aset Non TI
80	3050104003	Rak Besi	50	Abacus Dinding	11/11/2002	/	Baik	Aset Non TI
81	3050104003	Rak Besi	51	Abacus Dinding	11/11/2002	/	Baik	Aset Non TI
82	3050104003	Rak Besi	52	Abacus Dinding	11/11/2002	/	Baik	Aset Non TI
83	3050104003	Rak Besi	53	Abacus pintu kaca	11/11/2002	/	Baik	Aset Non TI
84	3050104003	Rak Besi	54	Abacus pintu kaca	11/11/2002	/	Baik	Aset Non TI
85	3050104003	Rak Besi	55	Rak besi	11/11/2002	/	Baik	Aset Non TI
86	3050104003	Rak Besi	56	Rak Besi	11/11/2002	/	Baik	Aset Non TI
87	3050104003	Rak Besi	57	Abacus Dinding	11/11/2002	/	Baik	Aset Non TI
88	3050104003	Rak Besi	58	Abacus Dinding	11/11/2002	/	Baik	Aset Non TI
89	3050104003	Rak Besi	59	Rak besi	11/11/2002	/	Baik	Aset Non TI
90	3050104003	Rak Besi	60	Abacus pintu kaca	11/11/2002	/	Baik	Aset Non TI
91	3050104003	Rak Besi	61	Abacus Dinding	11/11/2002	/	Baik	Aset Non TI
92	3050104003	Rak Besi	62	Rak besi Double Coloumn	11/11/2002	/	Baik	Aset Non TI
93	3050104003	Rak Besi	63	Abacus Dinding	11/11/2002	/	Baik	Aset Non TI
94	3050104003	Rak Besi	64	Rak besi	11/11/2002	/	Baik	Aset Non TI
95	3050104003	Rak Besi	65	Rak besi tanpa merk	11/11/2002	/	Baik	Aset Non TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
96	3050104003	Rak Besi	66	Abacus pintu kaca	11/11/2002	/	Baik	Aset Non TI
97	3050104003	Rak Besi	67	Rak Besi	11/11/2002	/	Baik	Aset Non TI
98	3050104003	Rak Besi	68	Rak besi Single Coloumn	11/11/2002	/	Baik	Aset Non TI
99	3050104003	Rak Besi	69	Rak besi	11/11/2002	/	Baik	Aset Non TI
100	3050104003	Rak Besi	70	Abacus pintu kaca	11/11/2002	/	Baik	Aset Non TI
101	3050104003	Rak Besi	71	Open Space Besi, Royal	11/11/2002	/	Baik	Aset Non TI
102	3050104003	Rak Besi	72	Rak Besi tanpa merk	11/11/2002	/	Baik	Aset Non TI
103	3050104003	Rak Besi	73	Abacus Dinding	11/11/2002	/	Baik	Aset Non TI
104	3050104003	Rak Besi	74	Rak besi Single Coloumn	11/11/2002	/	Baik	Aset Non TI
105	3050104003	Rak Besi	75	Lion/Steel Slotted Angle	9/1/2006	VI.3 / Data Center Gd Perpustakaan	Baik	Aset Non TI
106	3050104003	Rak Besi	76	Lion/Steel Slotted Angle	9/1/2006	VI.3 / Data Center Gd Perpustakaan	Baik	Aset Non TI
107	3050104003	Rak Besi	77	Lion/Steel Slotted Angle	9/1/2006	VI.3 / Data Center Gd Perpustakaan	Baik	Aset Non TI
108	3050104003	Rak Besi	78	Lion/Steel Slotted Angle	9/1/2006	VI.3 / Data Center Gd Perpustakaan	Baik	Aset Non TI
109	3050104003	Rak Besi	79	Lion/Steel Slotted Angle	9/1/2006	VI.3 / Data Center Gd Perpustakaan	Baik	Aset Non TI
110	3050104003	Rak Besi	80	Lion/Steel Slotted Angle	9/1/2006	VI.3 / Data Center Gd Perpustakaan	Baik	Aset Non TI
111	3050104003	Rak Besi	81	Rack 19	8/31/2009	/	Baik	Aset Non TI
112	3050104004	Rak Kayu	1	Custom	5/29/2017	/	Baik	Aset Non TI
113	3050104004	Rak Kayu	2	Custom	5/29/2017	A03 / Musholla	Baik	Aset Non TI
114	3050104005	Filing Cabinet Besi	2	Acroe	11/11/2002	B02-5 / R Direktur	Baik	Aset Non TI
115	3050104005	Filing Cabinet Besi	3	Bostinco	11/11/2002	A05-1 /	Baik	Aset Non TI
116	3050104005	Filing Cabinet Besi	4	Bostinco	11/11/2002	A05-2 /	Baik	Aset Non TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
117	3050104005	Filing Cabinet Besi	5	bostinco	11/11/2002	/	Baik	Aset Non TI
118	3050104005	Filing Cabinet Besi	6	bostinco	11/11/2002	/	Baik	Aset Non TI
119	3050104005	Filing Cabinet Besi	7	Elite	11/11/2002	B02 /	Baik	Aset Non TI
120	3050104005	Filing Cabinet Besi	8	Filling Cabinet bostinco	11/11/2002	/	Baik	Aset Non TI
121	3050104005	Filing Cabinet Besi	9	Bostinco	11/11/2002	/	Baik	Aset Non TI
122	3050104005	Filing Cabinet Besi	10	Bostinco	11/11/2002	/	Baik	Aset Non TI
123	3050104005	Filing Cabinet Besi	12	VIP	2/24/2012	/	Baik	Aset Non TI
124	3050104007	Brandkas	1		1/1/2003	B02 / R Keu & Adm	Baik	Aset Non TI
125	3050104012	Compact Rolling	1	Koper Pelican 1650 13.65kg	12/31/2017	B03-1 / Sekretariat SNMPTN	Baik	Aset Non TI
126	3050104012	Compact Rolling	2	Koper Pelican 1650 13.65kg	12/31/2017	B03-1 / Sekretariat SNMPTN	Baik	Aset Non TI
127	3050104012	Compact Rolling	3	Koper Pelican 1560 Small case	12/31/2017	B03-1 / Sekretariat SNMPTN	Baik	Aset Non TI
128	3050104014	Mobile File	1	Informa	12/11/2018	A05 / R Layanan TSI	Baik	Aset Non TI
129	3050104014	Mobile File	2	Informa	12/11/2018	A05 / R Layanan TSI	Baik	Aset Non TI
130	3050104014	Mobile File	3	Informa	12/11/2018	B01-4 / R Kasubdit IKTI	Baik	Aset Non TI
131	3050104014	Mobile File	4	Informa	12/11/2018	B02 / R Keu & Adm	Baik	Aset Non TI
132	3050104014	Mobile File	5	Informa	12/11/2018	B02-2 / R Staf Bangsi	Baik	Aset Non TI
133	3050104014	Mobile File	6	Informa	12/11/2018	B02-2 / R Staf Bangsi	Baik	Aset Non TI
134	3050104014	Mobile File	7	Informa	12/11/2018	B02-2 / R Staf Bangsi	Baik	Aset Non TI
135	3050104014	Mobile File	8	Informa	12/11/2018	B02-2 / R Staf Bangsi	Baik	Aset Non TI
136	3050104014	Mobile File	9	Informa	12/11/2018	B02-2 / R Staf Bangsi	Baik	Aset Non TI
137	3050104014	Mobile File	10	Informa	12/11/2018	B02-2 / R Staf Bangsi	Baik	Aset Non TI
138	3050104014	Mobile File	11	Informa	12/11/2018	B02-2 / R Staf Bangsi	Baik	Aset Non TI
139	3050104014	Mobile File	12	Informa	12/11/2018	B02-2 / R Staf Bangsi	Baik	Aset Non TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
140	3050104014	Mobile File	13	Informa	12/11/2018	B02-2 / R Staf Bangsi	Baik	Aset Non TI
141	3050104015	Locker	1	Inform	3/22/2017	A04 / R Serba Guna	Baik	Aset Non TI
142	3050104015	Locker	3	Informa	12/11/2018	B01-3 / R Rapat IKTI	Baik	Aset Non TI
143	3050105001	Tabung Pemadam Api	1	ECO	11/11/2002	/	Baik	Aset TI
144	3050105001	Tabung Pemadam Api	2	Appron AP -10 H	11/11/2002	/	Baik	Aset TI
145	3050105001	Tabung Pemadam Api	3	Worlmad	11/11/2002	/	Baik	Aset TI
146	3050105001	Tabung Pemadam Api	4	APPRON AP 400 H, Beroda	11/11/2002	/	Rusak	Aset TI
147	3050105001	Tabung Pemadam Api	5		11/11/2002	/	Baik	Aset TI
148	3050105001	Tabung Pemadam Api	6	APPRON AP 6 H	11/11/2002	/	Baik	Aset TI
149	3050105001	Tabung Pemadam Api	7	APPRON AP 6 H	11/11/2002	/	Baik	Aset TI
150	3050105001	Tabung Pemadam Api	8	APPRON AP 6 H	11/11/2002	/	Baik	Aset TI
151	3050105001	Tabung Pemadam Api	9	APPRON AP 6 H	11/11/2002	/	Baik	Aset TI
152	3050105001	Tabung Pemadam Api	10		11/11/2002	/	Baik	Aset TI
153	3050105001	Tabung Pemadam Api	11	Appron AP 10 H	11/11/2002	/	Baik	Aset TI
154	3050105001	Tabung Pemadam Api	12	Swordsman	11/11/2002	/	Baik	Aset TI
155	3050105001	Tabung Pemadam Api	13	APPRON AP 400 H, Beroda	11/11/2002	/	Rusak	Aset TI
156	3050105001	Tabung Pemadam Api	14	Appron AP 10 H	11/11/2002	/	Baik	Aset TI
157	3050105001	Tabung Pemadam Api	15	Appron AP 10 H	11/11/2002	/	Baik	Aset TI
158	3050105001	Tabung Pemadam Api	16	ECO	11/11/2002	/	Baik	Aset TI
159	3050105001	Tabung Pemadam Api	17	Blue -Benetron 5 kg	9/17/2018	A04 / R Serbaguna	Baik	Aset TI
160	3050105001	Tabung Pemadam Api	18	Blue -Benetron 5 kg	9/17/2018	A05 / R Layanan TSI	Baik	Aset TI
161	3050105001	Tabung Pemadam Api	19	Blue -Benetron 5 kg	9/17/2018	B01 / R. IKTI	Baik	Aset TI
162	3050105001	Tabung Pemadam Api	20	Blue -Benetron 5 kg	9/17/2018	B00 / Selasar Selatan	Baik	Aset TI
163	3050105007	CCTV - Camera Control Television System	1	Avtech	4/17/2013	/	Rusak	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
164	3050105007	CCTV - Camera Control Television System	2	Hikvision	12/28/2018	/	Baik	Aset TI
165	3050105007	CCTV - Camera Control Television System	3	Hikvision	12/28/2018	/	Baik	Aset TI
166	3050105007	CCTV - Camera Control Television System	4	Hikvision	12/28/2018	/	Baik	Aset TI
167	3050105007	CCTV - Camera Control Television System	5	Hikvision	12/28/2018	/	Baik	Aset TI
168	3050105007	CCTV - Camera Control Television System	6	Hikvision	12/28/2018	/	Baik	Aset TI
169	3050105007	CCTV - Camera Control Television System	7	Hikvision	12/28/2018	/	Baik	Aset TI
170	3050105007	CCTV - Camera Control Television System	8	Hikvision	12/28/2018	/	Baik	Aset TI
171	3050105007	CCTV - Camera Control Television System	9	Hikvision	12/28/2018	/	Baik	Aset TI
172	3050105007	CCTV - Camera Control Television System	10	Hikvision	12/28/2018	/	Baik	Aset TI
173	3050105007	CCTV - Camera Control Television System	11	Hikvision	12/28/2018	/	Baik	Aset TI
174	3050105007	CCTV - Camera Control Television System	12	Hikvision	12/28/2018	/	Baik	Aset TI
175	3050105007	CCTV - Camera Control Television System	13	Hikvision	12/28/2018	/	Baik	Aset TI
176	3050105007	CCTV - Camera Control Television System	14	Hikvision	12/28/2018	/	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
177	3050105007	CCTV - Camera Control Television System	15	Hikvision	12/28/2018	/	Baik	Aset TI
178	3050105007	CCTV - Camera Control Television System	16	Hikvision	12/28/2018	/	Baik	Aset TI
179	3050105007	CCTV - Camera Control Television System	17	Hikvision	12/28/2018	/	Baik	Aset TI
180	3050105007	CCTV - Camera Control Television System	18	Hikvision	12/28/2018	/	Baik	Aset TI
181	3050105007	CCTV - Camera Control Television System	19	Hikvision	12/28/2018	/	Baik	Aset TI
182	3050105007	CCTV - Camera Control Television System	20	Hikvision	12/28/2018	/	Baik	Aset TI
183	3050105007	CCTV - Camera Control Television System	21	Hikvision	12/28/2018	/	Baik	Aset TI
184	3050105007	CCTV - Camera Control Television System	22	Hikvision	12/28/2018	/	Baik	Aset TI
185	3050105007	CCTV - Camera Control Television System	23	Hikvision	12/28/2018	/	Baik	Aset TI
186	3050105007	CCTV - Camera Control Television System	24	Hikvision	12/28/2018	/	Baik	Aset TI
187	3050105007	CCTV - Camera Control Television System	25	Hikvision	12/28/2018	/	Baik	Aset TI
188	3050105007	CCTV - Camera Control Television System	26	Hikvision	12/28/2018	/	Baik	Aset TI
189	3050105007	CCTV - Camera Control Television System	27	Hikvision	12/28/2018	/	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
190	3050105007	CCTV - Camera Control Television System	28	Hikvision	12/28/2018	/	Baik	Aset TI
191	3050105007	CCTV - Camera Control Television System	29	Hikvision	12/28/2018	/	Baik	Aset TI
192	3050105007	CCTV - Camera Control Television System	30	Hikvision	12/28/2018	/	Baik	Aset TI
193	3050105007	CCTV - Camera Control Television System	31	Hikvision	12/28/2018	/	Baik	Aset TI
194	3050105007	CCTV - Camera Control Television System	32	Hikvision	12/28/2018	/	Baik	Aset TI
195	3050105007	CCTV - Camera Control Television System	33	Hikvision	12/28/2018	/	Baik	Aset TI
196	3050105007	CCTV - Camera Control Television System	34	Hikvision	12/28/2018	/	Baik	Aset TI
197	3050105007	CCTV - Camera Control Television System	35	Hikvision	12/28/2018	/	Baik	Aset TI
198	3050105007	CCTV - Camera Control Television System	36	Hikvision	12/28/2018	/	Baik	Aset TI
199	3050105007	CCTV - Camera Control Television System	37	Hikvision	12/28/2018	/	Baik	Aset TI
200	3050105007	CCTV - Camera Control Television System	38	Hikvision	12/28/2018	/	Baik	Aset TI
201	3050105007	CCTV - Camera Control Television System	39	Hikvision	12/28/2018	/	Baik	Aset TI
202	3050105010	White Board	4	Whiteboard	11/11/2002	/	Rusak	Aset Non TI
203	3050105010	White Board	6	Whiteboard	11/11/2002	/	Rusak	Aset Non TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
204	3050105010	White Board	7	Sakana	12/6/2013	A04-1 /	Baik	Aset Non TI
205	3050105010	White Board	8	Hanging Board	12/19/2017	A05-1 / R Kasubdit Yansi	Baik	Aset Non TI
206	3050105010	White Board	9	Hanging Board	12/19/2017	A05-2 / R Kasi Ldatin	Baik	Aset Non TI
207	3050105010	White Board	10	Hanging Board	12/19/2017	B01 / R. Staf IKTI	Baik	Aset Non TI
208	3050105010	White Board	11	Hanging Board	12/19/2017	B02-4 / R. Kasubdit Bangsi	Baik	Aset Non TI
209	3050105015	Alat Penghancur Kertas	1	Secure	8/11/2017	B02-4 /	Baik	Aset Non TI
210	3050105015	Alat Penghancur Kertas	2	Panasonic MP - S50	11/11/2002	B02-3 /	Baik	Aset Non TI
211	3050105015	Alat Penghancur Kertas	3	Krisbow S433	12/14/2017	B02-3 /	Baik	Aset Non TI
212	3050105015	Alat Penghancur Kertas	4	Expert TypeGEMET 320 C	12/31/2017	/	Baik	Aset Non TI
213	3050105015	Alat Penghancur Kertas	5	Secure Paper Shredder MAXI 25CCM	12/31/2017	/	Baik	Aset Non TI
214	3050105038	Laser Pointer	1	Infiniter Green Laser Pointer LR-12GR Pro	12/31/2017	/	Baik	Aset Non TI
215	3050105038	Laser Pointer	2	Infiniter Green Laser Pointer LR-12GR Pro	12/31/2017	/	Baik	Aset Non TI
216	3050105048	LCD Projector/Infocus	1	Infocus	5/29/2017	A04-1 / R Lab1	Baik	Aset TI
217	3050105048	LCD Projector/Infocus	2	Infocus	5/29/2017	B02-3 / R Rapat Layanan TSI	Baik	Aset TI
218	3050105048	LCD Projector/Infocus	3	Infocus	5/29/2017	B02-3 / R Rapat Pusdatin	Baik	Aset TI
219	3050105048	LCD Projector/Infocus	4	Samsung 732 NW	5/29/2009	A05 /	Rusak	Aset TI
220	3050105048	LCD Projector/Infocus	5	LCD Projector	12/17/2012	/	Rusak	Aset TI
221	3050105048	LCD Projector/Infocus	6	LCD Projector	12/17/2012	/	Rusak	Aset TI
222	3050105048	LCD Projector/Infocus	7	Indisium	12/3/2013	A05 / R Layanan TSI	Baik	Aset TI
223	3050105048	LCD Projector/Infocus	8	Philips Pico Pix ppx 4935	12/31/2017	B03-1 / R Sekretariat SBMPTN	Baik	Aset TI
224	3050105048	LCD Projector/Infocus	9	Philips Pico Pix ppx 4935	12/31/2017	B03-1 / R Sekretariat SBMPTN	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
225	3050105058	Focusing Screen/Layar LCD Projector	1	Projection Screens	12/17/2012	/	Rusak	Aset Non TI
226	3050105058	Focusing Screen/Layar LCD Projector	2	Projection Screens	12/17/2012	/	Rusak	Aset Non TI
227	3050105073	Alat Sidik Jari	1	FInger Prnt	11/28/2014	/	Baik	Aset TI
228	3050105999	Perkakas Kantor Lainnya	3	whiteboard elektrik/ Panaboard	12/31/2005	B03 / R. Validasi	Baik	Aset Non TI
229	3050201001	Meja Kerja Besi/Metal	1	Meja printer besi	11/11/2002	B00 / Selasar Selatan	Baik	Aset Non TI
230	3050201001	Meja Kerja Besi/Metal	2	Meja printer besi	11/11/2002	B00 / Selasar Selatan	Baik	Aset Non TI
231	3050201002	Meja Kerja Kayu	2	Meja printer	11/11/2002	A05 / R Layanan TSI	Baik	Aset Non TI
232	3050201002	Meja Kerja Kayu	4	Kayu	11/11/2002	/	Baik	Aset Non TI
233	3050201002	Meja Kerja Kayu	5	Kayu	11/11/2002	/	Baik	Aset Non TI
234	3050201002	Meja Kerja Kayu	7	Meja printer kayu	11/11/2002	B02-4 /	Baik	Aset Non TI
235	3050201002	Meja Kerja Kayu	8	Kayu	11/11/2002	B02-4 /	Baik	Aset Non TI
236	3050201002	Meja Kerja Kayu	9	Meja Kayu	11/11/2002	/	Baik	Aset Non TI
237	3050201002	Meja Kerja Kayu	10	Meja kayu	11/11/2002	/	Baik	Aset Non TI
238	3050201002	Meja Kerja Kayu	12	Kayu	11/11/2002	/	Baik	Aset Non TI
239	3050201002	Meja Kerja Kayu	13	Meja Kayu	11/11/2002	/	Baik	Aset Non TI
240	3050201002	Meja Kerja Kayu	14	1 Biro	11/11/2002	A05-2 /	Baik	Aset Non TI
241	3050201002	Meja Kerja Kayu	15	Ligna 1/2 biro	11/11/2002	B03 / R Validasi	Baik	Aset Non TI
242	3050201002	Meja Kerja Kayu	17	Ligna Full biro	11/11/2002	B02 / R Keu & Adm	Baik	Aset Non TI
243	3050201002	Meja Kerja Kayu	18	Meja sidang	11/11/2002	/	Baik	Aset Non TI
244	3050201002	Meja Kerja Kayu	19	Meja Kayu	11/11/2002	/	Baik	Aset Non TI
245	3050201002	Meja Kerja Kayu	20	Meja Kayu	11/11/2002	/	Baik	Aset Non TI
246	3050201002	Meja Kerja Kayu	21	Meja kayu	11/11/2002	/	Baik	Aset Non TI
247	3050201002	Meja Kerja Kayu	23	1/2 biro	11/11/2002	/	Baik	Aset Non TI
248	3050201002	Meja Kerja Kayu	24	Meja Kayu	11/11/2002	/	Baik	Aset Non TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
249	3050201002	Meja Kerja Kayu	25	Meja sidang	11/11/2002	/	Baik	Aset Non TI
250	3050201002	Meja Kerja Kayu	28		11/11/2002	B02 /	Baik	Aset Non TI
251	3050201002	Meja Kerja Kayu	29	Meja sidang	11/11/2002	/	Baik	Aset Non TI
252	3050201002	Meja Kerja Kayu	32	Meja sidang	11/11/2002	/	Baik	Aset Non TI
253	3050201002	Meja Kerja Kayu	33	Meja sidang	11/11/2002	/	Baik	Aset Non TI
254	3050201002	Meja Kerja Kayu	35	1/2 Biro	11/11/2002	/	Baik	Aset Non TI
255	3050201002	Meja Kerja Kayu	36	Meja sidang	11/11/2002	/	Baik	Aset Non TI
256	3050201002	Meja Kerja Kayu	37	Meja sidang	11/11/2002	/	Baik	Aset Non TI
257	3050201002	Meja Kerja Kayu	38	Meja Kerja	11/11/2002	/	Baik	Aset Non TI
258	3050201002	Meja Kerja Kayu	39	Ligna Full Biro	11/11/2002	B02 / R Keu & Adm	Baik	Aset Non TI
259	3050201002	Meja Kerja Kayu	40	Ligna 1 biro	11/11/2002	B03 / R Validasi	Baik	Aset Non TI
260	3050201002	Meja Kerja Kayu	42	Meja 1 Biro	11/11/2002	/	Baik	Aset Non TI
261	3050201002	Meja Kerja Kayu	43	1/2 biro	11/11/2002	/	Baik	Aset Non TI
262	3050201003	Kursi Besi/Metal	1	Informa	5/23/2017	B02-3 / R Rapat Bangsi	Baik	Aset Non TI
263	3050201003	Kursi Besi/Metal	2	Informa	5/23/2017	B02-3 / R Rapat Bangsi	Baik	Aset Non TI
264	3050201003	Kursi Besi/Metal	3	Informa	5/23/2017	B02-3 / R Rapat Bangsi	Baik	Aset Non TI
265	3050201003	Kursi Besi/Metal	4	Informa	5/23/2017	B02-3 / R Rapat Bangsi	Baik	Aset Non TI
266	3050201003	Kursi Besi/Metal	5	Informa	5/23/2017	B02-3 / R Rapat Bangsi	Baik	Aset Non TI
267	3050201003	Kursi Besi/Metal	6	Informa	5/23/2017	B02-3 / R Rapat Bangsi	Baik	Aset Non TI
268	3050201003	Kursi Besi/Metal	7	Informa	5/23/2017	B02-3 / R Rapat Bangsi	Baik	Aset Non TI
269	3050201003	Kursi Besi/Metal	8	Informa	5/23/2017	B02-3 / R Rapat Bangsi	Baik	Aset Non TI
270	3050201003	Kursi Besi/Metal	9	Informa	5/23/2017	B02-3 / R Rapat Bangsi	Baik	Aset Non TI
271	3050201003	Kursi Besi/Metal	10	Informa	5/23/2017	B02-3 / R Rapat Bangsi	Baik	Aset Non TI
272	3050201003	Kursi Besi/Metal	11	Informa	5/23/2017	B02-3 / R Rapat Bangsi	Baik	Aset Non TI
273	3050201003	Kursi Besi/Metal	12	Informa	5/23/2017	B02-3 / R Rapat Bangsi	Baik	Aset Non TI
274	3050201003	Kursi Besi/Metal	13	Informa	5/23/2017	B02-3 / R Rapat Bangsi	Baik	Aset Non TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
275	3050201003	Kursi Besi/Metal	14	Informa	5/23/2017	A04-1 / R Pelatihan1	Baik	Aset Non TI
276	3050201003	Kursi Besi/Metal	15	Informa	5/23/2017	B01 / R. IKTI	Baik	Aset Non TI
277	3050201003	Kursi Besi/Metal	16	Informa	5/23/2017	B01 / R. IKTI	Baik	Aset Non TI
278	3050201003	Kursi Besi/Metal	17	Informa	5/23/2017	B01 / R. IKTI	Baik	Aset Non TI
279	3050201003	Kursi Besi/Metal	18	Informa	5/23/2017	B01 / R. IKTI	Baik	Aset Non TI
280	3050201003	Kursi Besi/Metal	19	Informa	5/23/2017	B01 / R. IKTI	Baik	Aset Non TI
281	3050201003	Kursi Besi/Metal	20	Informa	5/23/2017	B01 / R. IKTI	Baik	Aset Non TI
282	3050201003	Kursi Besi/Metal	21	Informa	5/23/2017	B01 / R. IKTI	Baik	Aset Non TI
283	3050201003	Kursi Besi/Metal	22	Informa	5/23/2017	B01 / R. IKTI	Baik	Aset Non TI
284	3050201003	Kursi Besi/Metal	23	Informa	5/23/2017	B01-4 / R Kasubdit IKTI	Baik	Aset Non TI
285	3050201003	Kursi Besi/Metal	24	Informa	5/23/2017	B01-4 / R Kasubdit IKTI	Baik	Aset Non TI
286	3050201003	Kursi Besi/Metal	26		11/11/2002	/	Baik	Aset Non TI
287	3050201003	Kursi Besi/Metal	30	Chitose	11/11/2002	/	Baik	Aset Non TI
288	3050201003	Kursi Besi/Metal	33		11/11/2002	/	Baik	Aset Non TI
289	3050201003	Kursi Besi/Metal	34		11/11/2002	/	Baik	Aset Non TI
290	3050201003	Kursi Besi/Metal	36		11/11/2002	/	Baik	Aset Non TI
291	3050201003	Kursi Besi/Metal	37	Isebel 150 T	11/11/2002	/	Baik	Aset Non TI
292	3050201003	Kursi Besi/Metal	42	Isebel 150 T	11/11/2002	/	Baik	Aset Non TI
293	3050201003	Kursi Besi/Metal	43		11/11/2002	/	Baik	Aset Non TI
294	3050201003	Kursi Besi/Metal	44	Chitose	11/11/2002	/	Baik	Aset Non TI
295	3050201003	Kursi Besi/Metal	45	Isebel 150 T	11/11/2002	/	Baik	Aset Non TI
296	3050201003	Kursi Besi/Metal	49		11/11/2002	/	Baik	Aset Non TI
297	3050201003	Kursi Besi/Metal	51	Isebel 150 T	11/11/2002	/	Baik	Aset Non TI
298	3050201003	Kursi Besi/Metal	54	Rakuda 150 T	11/11/2002	A04 / R Serbaguna	Baik	Aset Non TI
299	3050201003	Kursi Besi/Metal	55	Rakuda 150 T	11/11/2002	A04 / R Serbaguna	Baik	Aset Non TI
300	3050201003	Kursi Besi/Metal	56	Rakuda 150 T	11/11/2002	A04 / R Serbaguna	Baik	Aset Non TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
301	3050201003	Kursi Besi/Metal	57	Rakuda 150 T	11/11/2002	A04 / R Serbaguna	Baik	Aset Non TI
302	3050201003	Kursi Besi/Metal	58		11/11/2002	/	Baik	Aset Non TI
303	3050201003	Kursi Besi/Metal	64	Isebel 150 T	11/11/2002	/	Baik	Aset Non TI
304	3050201003	Kursi Besi/Metal	67		11/11/2002	/	Baik	Aset Non TI
305	3050201003	Kursi Besi/Metal	70		11/11/2002	/	Baik	Aset Non TI
306	3050201003	Kursi Besi/Metal	71		11/11/2002	/	Baik	Aset Non TI
307	3050201003	Kursi Besi/Metal	72	Rakuda 150 T	11/11/2002	/	Baik	Aset Non TI
308	3050201003	Kursi Besi/Metal	73	Rakuda 150 T	11/11/2002	/	Baik	Aset Non TI
309	3050201003	Kursi Besi/Metal	74		11/11/2002	/	Baik	Aset Non TI
310	3050201003	Kursi Besi/Metal	75	Rakuda 150 T	11/11/2002	/	Baik	Aset Non TI
311	3050201003	Kursi Besi/Metal	76	Isebel 150 T	11/11/2002	/	Rusak	Aset Non TI
312	3050201003	Kursi Besi/Metal	77		11/11/2002	/	Baik	Aset Non TI
313	3050201003	Kursi Besi/Metal	78		11/11/2002	/	Baik	Aset Non TI
314	3050201003	Kursi Besi/Metal	82	Isebel 150 T	11/11/2002	/	Rusak	Aset Non TI
315	3050201003	Kursi Besi/Metal	84	Kursi Putar Chitose	11/11/2002	/	Baik	Aset Non TI
316	3050201003	Kursi Besi/Metal	86	Isebel 150 T	11/11/2002	/	Rusak	Aset Non TI
317	3050201003	Kursi Besi/Metal	87		11/11/2002	/	Baik	Aset Non TI
318	3050201003	Kursi Besi/Metal	88		11/11/2002	/	Baik	Aset Non TI
319	3050201003	Kursi Besi/Metal	94	Rakuda 150 T	11/11/2002	/	Baik	Aset Non TI
320	3050201003	Kursi Besi/Metal	95	Isebel 150 T	11/11/2002	/	Rusak	Aset Non TI
321	3050201003	Kursi Besi/Metal	96		11/11/2002	/	Rusak	Aset Non TI
322	3050201003	Kursi Besi/Metal	97		11/11/2002	/	Rusak	Aset Non TI
323	3050201003	Kursi Besi/Metal	98	Isebel 150 T	11/11/2002	/	Rusak	Aset Non TI
324	3050201003	Kursi Besi/Metal	99	Isebel 150 T	11/11/2002	/	Rusak	Aset Non TI
325	3050201003	Kursi Besi/Metal	103	Indachi	11/11/2002	/	Baik	Aset Non TI
326	3050201003	Kursi Besi/Metal	104		11/11/2002	/	Baik	Aset Non TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
327	3050201003	Kursi Besi/Metal	105	Rakuda 150 T	11/11/2002	/	Baik	Aset Non TI
328	3050201003	Kursi Besi/Metal	106	Isebel 150 T	11/11/2002	/	Baik	Aset Non TI
329	3050201003	Kursi Besi/Metal	107	Kursi Lipat	11/11/2002	/	Baik	Aset Non TI
330	3050201003	Kursi Besi/Metal	109		11/11/2002	/	Baik	Aset Non TI
331	3050201003	Kursi Besi/Metal	110	Isebel 150 T	11/11/2002	/	Baik	Aset Non TI
332	3050201003	Kursi Besi/Metal	111	Isebel 150 T	11/11/2002	/	Baik	Aset Non TI
333	3050201003	Kursi Besi/Metal	113	Kursi Putar Bostinco	11/11/2002	/	Rusak	Aset Non TI
334	3050201003	Kursi Besi/Metal	116		11/11/2002	/	Baik	Aset Non TI
335	3050201003	Kursi Besi/Metal	119	Rakuda 150 T	11/11/2002	/	Rusak	Aset Non TI
336	3050201003	Kursi Besi/Metal	120	Rakuda 150 T	11/11/2002	/	Rusak	Aset Non TI
337	3050201003	Kursi Besi/Metal	121	Isebel 150 T	11/11/2002	/	Rusak	Aset Non TI
338	3050201003	Kursi Besi/Metal	122	Kursi Putar Bostinco	11/11/2002	/	Baik	Aset Non TI
339	3050201003	Kursi Besi/Metal	123		11/11/2002	/	Baik	Aset Non TI
340	3050201003	Kursi Besi/Metal	125	Kursi Putar Bostinco	11/11/2002	/	Baik	Aset Non TI
341	3050201003	Kursi Besi/Metal	127		11/11/2002	/	Baik	Aset Non TI
342	3050201003	Kursi Besi/Metal	130		11/11/2002	/	Baik	Aset Non TI
343	3050201003	Kursi Besi/Metal	132	Kursi Lipat Phonix	11/11/2002	/	Rusak	Aset Non TI
344	3050201003	Kursi Besi/Metal	134	Kursi lipat Phonix	11/11/2002	/	Rusak	Aset Non TI
345	3050201003	Kursi Besi/Metal	136	Kursi Lipat	11/11/2002	/	Baik	Aset Non TI
346	3050201003	Kursi Besi/Metal	143	Kursi Lipat	11/11/2002	/	Baik	Aset Non TI
347	3050201003	Kursi Besi/Metal	144	Kursi lipat	11/11/2002	/	Baik	Aset Non TI
348	3050201003	Kursi Besi/Metal	146	Kursi Lipat	11/11/2002	/	Baik	Aset Non TI
349	3050201003	Kursi Besi/Metal	148	Kursi Lipat	11/11/2002	/	Baik	Aset Non TI
350	3050201003	Kursi Besi/Metal	152	Kursi lipat tanpa merk	11/11/2002	/	Baik	Aset Non TI
351	3050201003	Kursi Besi/Metal	153	Kursi lipat tanpa merk	11/11/2002	/	Baik	Aset Non TI
352	3050201003	Kursi Besi/Metal	154	Kursi lipat tanpa merk	11/11/2002	/	Baik	Aset Non TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
353	3050201003	Kursi Besi/Metal	163	Kursi Lipat	11/11/2002	/	Rusak	Aset Non TI
354	3050201003	Kursi Besi/Metal	166	Kursi Rakuda	11/11/2002	/	Rusak	Aset Non TI
355	3050201003	Kursi Besi/Metal	169	Kursi Lipat	11/11/2002	/	Rusak	Aset Non TI
356	3050201003	Kursi Besi/Metal	172	Informa Zach Staff Chair	12/19/2017	A05-1 / R Kasubdit Yansi	Baik	Aset Non TI
357	3050201003	Kursi Besi/Metal	173	Informa Zach Staff Chair	12/19/2017	A05-1 / R Kasubdit Yansi	Baik	Aset Non TI
358	3050201003	Kursi Besi/Metal	174	Informa Zach Staff Chair	12/19/2017	A05-2 / Kasi Ldatin	Baik	Aset Non TI
359	3050201003	Kursi Besi/Metal	175	Informa Zach Staff Chair	12/19/2017	A05-2 / Kasi Ldatin	Baik	Aset Non TI
360	3050201003	Kursi Besi/Metal	176	Informa Zach Staff Chair	12/19/2017	A05 / R Layanan TSI	Baik	Aset Non TI
361	3050201003	Kursi Besi/Metal	177	Informa Zach Staff Chair	12/19/2017	A05 / R Layanan TSI	Baik	Aset Non TI
362	3050201003	Kursi Besi/Metal	178	Informa Zach Staff Chair	12/19/2017	A05 / R Layanan TSI	Baik	Aset Non TI
363	3050201003	Kursi Besi/Metal	179	Informa Zach Staff Chair	12/19/2017	A05 / R Layanan TSI	Baik	Aset Non TI
364	3050201003	Kursi Besi/Metal	180	Informa Zach Staff Chair	12/19/2017	A05 / R Layanan TSI	Baik	Aset Non TI
365	3050201003	Kursi Besi/Metal	181	Informa Zach Staff Chair	12/19/2017	A05-3 / R Rapat Yansi	Baik	Aset Non TI
366	3050201003	Kursi Besi/Metal	182	Informa Zach Staff Chair	12/19/2017	A05-3 / R Rapat Yansi	Baik	Aset Non TI
367	3050201003	Kursi Besi/Metal	183	Informa Zach Staff Chair	12/19/2017	A05-3 / R Rapat Yansi	Baik	Aset Non TI
368	3050201003	Kursi Besi/Metal	184	Informa Zach Staff Chair	12/19/2017	A05-3 / R Rapat Yansi	Baik	Aset Non TI
369	3050201003	Kursi Besi/Metal	185	Informa Zach Staff Chair	12/19/2017	A05-3 / R Rapat Yansi	Baik	Aset Non TI
370	3050201003	Kursi Besi/Metal	186	Informa Zach Staff Chair	12/19/2017	A05-3 / R Rapat Yansi	Baik	Aset Non TI
371	3050201003	Kursi Besi/Metal	187	Informa Zach Staff Chair	12/19/2017	A05-3 / R Rapat Yansi	Baik	Aset Non TI
372	3050201003	Kursi Besi/Metal	188	Informa Zach Staff Chair	12/19/2017	A05-3 / R Rapat Yansi	Baik	Aset Non TI
373	3050201003	Kursi Besi/Metal	189	Informa Zach Staff Chair	12/19/2017	A05-3 / R Rapat Yansi	Baik	Aset Non TI
374	3050201003	Kursi Besi/Metal	190	Informa Zach Staff Chair	12/19/2017	A05-3 / R Rapat Yansi	Baik	Aset Non TI
375	3050201003	Kursi Besi/Metal	191	Informa Zach Staff Chair	12/19/2017	A05-3 / R Rapat Yansi	Baik	Aset Non TI
376	3050201003	Kursi Besi/Metal	192	Informa Zach Staff Chair	12/19/2017	A05-3 / R Rapat Yansi	Baik	Aset Non TI
377	3050201003	Kursi Besi/Metal	193	Informa Zach Staff Chair	12/19/2017	A05-3 / R Rapat Yansi	Baik	Aset Non TI
378	3050201003	Kursi Besi/Metal	194	Informa Zach Staff Chair	12/19/2017	A05-3 / R Rapat Yansi	Baik	Aset Non TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
379	3050201003	Kursi Besi/Metal	195	Informa Zach Staff Chair	12/19/2017	A05-3 / R Rapat Yansi	Baik	Aset Non TI
380	3050201003	Kursi Besi/Metal	196	Informa Zach Staff Chair	12/19/2017	A05 / R Layanan TSI	Baik	Aset Non TI
381	3050201003	Kursi Besi/Metal	197	Informa Zach Staff Chair	12/19/2017	B02 / R Keu & Adm	Baik	Aset Non TI
382	3050201003	Kursi Besi/Metal	198	Informa Zach Staff Chair	12/19/2017	B02 / R Keu & Adm	Baik	Aset Non TI
383	3050201003	Kursi Besi/Metal	199	Informa Zach Staff Chair	12/19/2017	B02 / R Keu & Adm	Baik	Aset Non TI
384	3050201003	Kursi Besi/Metal	200	Informa Zach Staff Chair	12/19/2017	B02 / R Keu & Adm	Baik	Aset Non TI
385	3050201003	Kursi Besi/Metal	201	Informa Zach Staff Chair	12/19/2017	B02-3 / R Rapat Bangsi	Baik	Aset Non TI
386	3050201003	Kursi Besi/Metal	202	Informa Zach Staff Chair	12/19/2017	B02-3 / R Rapat Bangsi	Baik	Aset Non TI
387	3050201003	Kursi Besi/Metal	203	Informa Zach Staff Chair	12/19/2017	B02-2 / R Staf Bangsi	Baik	Aset Non TI
388	3050201003	Kursi Besi/Metal	204	Informa Zach Staff Chair	12/19/2017	B02-2 / R Staf Bangsi	Baik	Aset Non TI
389	3050201003	Kursi Besi/Metal	205	Informa Zach Staff Chair	12/19/2017	B02-2 / R Staf Bangsi	Baik	Aset Non TI
390	3050201003	Kursi Besi/Metal	206	Informa Zach Staff Chair	12/19/2017	B02-2 / R Staf Bangsi	Baik	Aset Non TI
391	3050201003	Kursi Besi/Metal	207	Informa Zach Staff Chair	12/19/2017	B02-2 / R Staf Bangsi	Baik	Aset Non TI
392	3050201003	Kursi Besi/Metal	208	Informa Zach Staff Chair	12/19/2017	B02-2 / R Staf Bangsi	Baik	Aset Non TI
393	3050201003	Kursi Besi/Metal	209	Informa Zach Staff Chair	12/19/2017	B02-2 / R Staf Bangsi	Baik	Aset Non TI
394	3050201003	Kursi Besi/Metal	210	Informa Zach Staff Chair	12/19/2017	B02-2 / R Staf Bangsi	Baik	Aset Non TI
395	3050201003	Kursi Besi/Metal	211	Informa Zach Staff Chair	12/19/2017	B02-2 / R Staf Bangsi	Baik	Aset Non TI
396	3050201003	Kursi Besi/Metal	212	Informa Zach Staff Chair	12/19/2017	B02-2 / R Staf Bangsi	Baik	Aset Non TI
397	3050201003	Kursi Besi/Metal	213	Informa Zach Staff Chair	12/19/2017	B02-2 / R Staf Bangsi	Baik	Aset Non TI
398	3050201003	Kursi Besi/Metal	214	Informa Zach Staff Chair	12/19/2017	B02-2 / R Staf Bangsi	Baik	Aset Non TI
399	3050201003	Kursi Besi/Metal	215	Informa Zach Staff Chair	12/19/2017	A04-1 / R Pelatihan 1	Baik	Aset Non TI
400	3050201003	Kursi Besi/Metal	216	Informa Zach Staff Chair	12/19/2017	A04-1 / R Pelatihan 1	Baik	Aset Non TI
401	3050201003	Kursi Besi/Metal	217	Informa Zach Staff Chair	12/19/2017	A04-1 / R Pelatihan 1	Baik	Aset Non TI
402	3050201003	Kursi Besi/Metal	218	Informa Zach Staff Chair	12/19/2017	A04-1 / R Pelatihan 1	Baik	Aset Non TI
403	3050201003	Kursi Besi/Metal	219	Informa Zach Staff Chair	12/19/2017	A04-1 / R Pelatihan 1	Baik	Aset Non TI
404	3050201003	Kursi Besi/Metal	220	Informa Zach Staff Chair	12/19/2017	A04-1 / R Pelatihan 1	Baik	Aset Non TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
405	3050201003	Kursi Besi/Metal	221	Informa Zach Staff Chair	12/19/2017	A04-1 / R Pelatihan 1	Baik	Aset Non TI
406	3050201003	Kursi Besi/Metal	222	Informa Zach Staff Chair	12/19/2017	A04-1 / R Pelatihan 1	Baik	Aset Non TI
407	3050201003	Kursi Besi/Metal	223	Informa Zach Staff Chair	12/19/2017	A04-1 / R Pelatihan 1	Baik	Aset Non TI
408	3050201003	Kursi Besi/Metal	224		11/11/2002	/	Baik	Aset Non TI
409	3050201005	Sice	1	Kursi tamu	11/11/2002	A05-1 / R Kasubdit Yansi	Baik	Aset Non TI
410	3050201005	Sice	2	Sofa	1/1/2005	A05-2 / Kasi Ldatin	Baik	Aset Non TI
411	3050201006	Bangku Panjang Besi/Metal	1	Informa	3/22/2017	A05 / R Layanan TSI	Baik	Aset Non TI
412	3050201006	Bangku Panjang Besi/Metal	2	Informa	3/22/2017	A05 / R Layanan TSI	Baik	Aset Non TI
413	3050201006	Bangku Panjang Besi/Metal	3	Informa	3/22/2017	A05 / R Layanan TSI	Baik	Aset Non TI
414	3050201008	Meja Rapat	1	Victor MD 240	11/11/2002	B02-3 / R Rapat Bangsi	Baik	Aset Non TI
415	3050201008	Meja Rapat	3	Meja kayu	11/11/2002	/	Baik	Aset Non TI
416	3050201008	Meja Rapat	4	Meja sidang	11/11/2002	/	Baik	Aset Non TI
417	3050201008	Meja Rapat	5	Meja kayu	11/11/2002	/	Baik	Aset Non TI
418	3050201008	Meja Rapat	6	Meja rapat Highpoint	11/11/2002	/	Rusak	Aset Non TI
419	3050201008	Meja Rapat	7	Meja sidang	11/11/2002	/	Baik	Aset Non TI
420	3050201008	Meja Rapat	8	Meja sidang Kayu	11/11/2002	/	Baik	Aset Non TI
421	3050201008	Meja Rapat	9	Meja sidang Kayu	11/11/2002	/	Baik	Aset Non TI
422	3050201008	Meja Rapat	10	Victor MD 240	11/11/2002	B02-3 / R Rapat Bangsi	Baik	Aset Non TI
423	3050201008	Meja Rapat	11	Meja sidang	11/11/2002	/	Baik	Aset Non TI
424	3050201008	Meja Rapat	12	Meja sidang	11/11/2002	/	Baik	Aset Non TI
425	3050201009	Meja Komputer	1	Custom	5/29/2017	A04-2 / R Pelatihan 2	Baik	Aset Non TI
426	3050201009	Meja Komputer	2	Custom	5/29/2017	A04-2 / R Pelatihan 2	Baik	Aset Non TI
427	3050201009	Meja Komputer	3	Custom	5/29/2017	A04-2 / R Pelatihan 2	Baik	Aset Non TI
428	3050201009	Meja Komputer	4	Custom	5/29/2017	A04-2 / R Pelatihan 2	Baik	Aset Non TI
429	3050201009	Meja Komputer	5	Custom	5/29/2017	A04-2 / R Pelatihan 2	Baik	Aset Non TI
430	3050201009	Meja Komputer	6	Custom	5/29/2017	A04-2 / R Pelatihan 2	Baik	Aset Non TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
431	3050201009	Meja Komputer	7	Custom	5/29/2017	A04-3 / R Pelatihan 3	Baik	Aset Non TI
432	3050201009	Meja Komputer	8	Custom	5/29/2017	A04-3 / R Pelatihan 3	Baik	Aset Non TI
433	3050201009	Meja Komputer	9	Custom	5/29/2017	A04-3 / R Pelatihan 3	Baik	Aset Non TI
434	3050201009	Meja Komputer	10	Custom	5/29/2017	A04-3 / R Pelatihan 3	Baik	Aset Non TI
435	3050201009	Meja Komputer	11	Custom	5/29/2017	A04-3 / R Pelatihan 3	Baik	Aset Non TI
436	3050201009	Meja Komputer	12	Custom	5/29/2017	A04-3 / R Pelatihan 3	Baik	Aset Non TI
437	3050201009	Meja Komputer	14	Victor CD90	11/11/2002	B01 / R Staf IKTI	Baik	Aset Non TI
438	3050201009	Meja Komputer	17	Victor CD90	11/11/2002	B01 / R Staf IKTI	Baik	Aset Non TI
439	3050201009	Meja Komputer	18	Victor CD90	11/11/2002	B01 / R Staf IKTI	Baik	Aset Non TI
440	3050201009	Meja Komputer	20	Victor CD 90	11/11/2002	B01 / R Staf IKTI	Baik	Aset Non TI
441	3050201009	Meja Komputer	22	Victor CD 90	11/11/2002	B01 / R Staf IKTI	Baik	Aset Non TI
442	3050201009	Meja Komputer	23	Victor CD 90	11/11/2002	B01 / R Staf IKTI	Baik	Aset Non TI
443	3050201009	Meja Komputer	24	Victor CD 90	11/11/2002	B01 / R Staf IKTI	Baik	Aset Non TI
444	3050201009	Meja Komputer	26	Victor CD 90	11/11/2002	B01 / R Staf IKTI	Baik	Aset Non TI
445	3050201009	Meja Komputer	27	Victor CD 90	11/11/2002	B01 / R Staf IKTI	Baik	Aset Non TI
446	3050201009	Meja Komputer	28		11/11/2002	A04-1 / R Pelatihan 1	Baik	Aset Non TI
447	3050201009	Meja Komputer	29		11/11/2002	A04-1 / R Pelatihan 1	Rusak	Aset Non TI
448	3050201009	Meja Komputer	30	Meja Komputer	11/11/2002	A04-1 / R Pelatihan 1	Baik	Aset Non TI
449	3050201009	Meja Komputer	31		11/11/2002	A04-1 / R Pelatihan 1	Baik	Aset Non TI
450	3050201009	Meja Komputer	33	Victor CD 90	11/11/2002	/	Baik	Aset Non TI
451	3050201009	Meja Komputer	34	Victor CD 90	11/11/2002	A04-1 / R Pelatihan 1	Baik	Aset Non TI
452	3050201009	Meja Komputer	35	Victor CD 90	11/11/2002	A04-1 / R Pelatihan 1	Baik	Aset Non TI
453	3050201009	Meja Komputer	36		11/11/2002	A04-1 / R Pelatihan 1	Rusak	Aset Non TI
454	3050201009	Meja Komputer	37		11/11/2002	A04-1 / R Pelatihan 1	Baik	Aset Non TI
455	3050201009	Meja Komputer	38		11/11/2002	A04-1 / R Pelatihan 1	Rusak	Aset Non TI
456	3050201009	Meja Komputer	40	Victor CD 90	11/11/2002	A04-1 / R Pelatihan 1	Baik	Aset Non TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
457	3050201009	Meja Komputer	41		11/11/2002	/	Baik	Aset Non TI
458	3050201009	Meja Komputer	42	Victor CD120	11/11/2002	/	Baik	Aset Non TI
459	3050201009	Meja Komputer	43	Victor CD 90	11/11/2002	A04-1 / R Pelatihan 1	Baik	Aset Non TI
460	3050201009	Meja Komputer	45	Meja Komputer Kayu	11/11/2002	B02-4 /	Baik	Aset Non TI
461	3050201009	Meja Komputer	46	Victor CD 120	11/11/2002	/	Baik	Aset Non TI
462	3050201009	Meja Komputer	47	Victor CD120	11/11/2002	/	Baik	Aset Non TI
463	3050201009	Meja Komputer	48	Victor CD 90	11/11/2002	A04-1 / R Pelatihan 1	Baik	Aset Non TI
464	3050201009	Meja Komputer	49	Victor CD 90	11/11/2002	A04-1 / R Pelatihan 1	Baik	Aset Non TI
465	3050201009	Meja Komputer	50	Victor CD120	11/11/2002	/	Baik	Aset Non TI
466	3050201009	Meja Komputer	56	Victor CD 90	11/11/2002	A04-1 / R Pelatihan 1	Baik	Aset Non TI
467	3050201009	Meja Komputer	60	Victor CD120	11/11/2002	A04-1 / R Pelatihan 1	Baik	Aset Non TI
468	3050201009	Meja Komputer	67	Victor CD 90	11/11/2002	A04-1 / R Pelatihan 1	Baik	Aset Non TI
469	3050201009	Meja Komputer	68	Victor CD 90	11/11/2002	A04-1 / R Pelatihan 1	Baik	Aset Non TI
470	3050201009	Meja Komputer	69	Victor CD 90	11/11/2002	A04-1 / R Pelatihan 1	Baik	Aset Non TI
471	3050201009	Meja Komputer	70	Victor CD 90	11/11/2002	A04-1 / R Pelatihan 1	Baik	Aset Non TI
472	3050201009	Meja Komputer	76	Victor CD 90	11/11/2002	A04-1 / R Pelatihan 1	Baik	Aset Non TI
473	3050201009	Meja Komputer	77	Victor CD 120	11/11/2002	B01 / R. IKTI	Baik	Aset Non TI
474	3050201009	Meja Komputer	78	Victor CD 120	11/11/2002	B01 / R. IKTI	Baik	Aset Non TI
475	3050201009	Meja Komputer	80		11/11/2002	/	Baik	Aset Non TI
476	3050201009	Meja Komputer	83		11/11/2002	/	Baik	Aset Non TI
477	3050201009	Meja Komputer	84	Victor CD 90	11/11/2002	A04-1 / R Pelatihan 1	Baik	Aset Non TI
478	3050201009	Meja Komputer	85		11/11/2002	/	Baik	Aset Non TI
479	3050201009	Meja Komputer	86		11/11/2002	/	Baik	Aset Non TI
480	3050201009	Meja Komputer	89	Olympic	11/11/2002	/	Rusak	Aset Non TI
481	3050201009	Meja Komputer	90		11/11/2002	/	Baik	Aset Non TI
482	3050201009	Meja Komputer	91	Olympic	11/11/2002	/	Rusak	Aset Non TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
483	3050201009	Meja Komputer	92	Olympic	11/11/2002	/	Rusak	Aset Non TI
484	3050201009	Meja Komputer	93		11/11/2002	/	Baik	Aset Non TI
485	3050201009	Meja Komputer	94		11/11/2002	/	Baik	Aset Non TI
486	3050201009	Meja Komputer	95	Olympic	11/11/2002	/	Baik	Aset Non TI
487	3050201009	Meja Komputer	96	Olympic	11/11/2002	/	Baik	Aset Non TI
488	3050201009	Meja Komputer	100	tanpa merk	11/11/2002	/	Baik	Aset Non TI
489	3050201009	Meja Komputer	101		11/11/2002	/	Baik	Aset Non TI
490	3050201009	Meja Komputer	102	Olympic	11/11/2002	/	Baik	Aset Non TI
491	3050201009	Meja Komputer	103		11/11/2002	/	Baik	Aset Non TI
492	3050201009	Meja Komputer	104	Victor CD 90	11/11/2002	A04-1 / R Pelatihan 1	Baik	Aset Non TI
493	3050201009	Meja Komputer	105	Olympic	11/11/2002	B03 /	Baik	Aset Non TI
494	3050201009	Meja Komputer	106	Olympic	11/11/2002	B03 /	Baik	Aset Non TI
495	3050201009	Meja Komputer	107	Olympic	11/11/2002	B03 /	Baik	Aset Non TI
496	3050201009	Meja Komputer	108	Olympic	11/11/2002	B03 /	Baik	Aset Non TI
497	3050201009	Meja Komputer	109	Olympic	11/11/2002	B03 /	Baik	Aset Non TI
498	3050201009	Meja Komputer	110	Olympic	11/11/2002	B03 /	Baik	Aset Non TI
499	3050201009	Meja Komputer	111	Meja Komputer Kayu	11/11/2002	/	Baik	Aset Non TI
500	3050201009	Meja Komputer	112	Olympic	11/11/2002	/	Rusak	Aset Non TI
501	3050201009	Meja Komputer	113	Olympic	11/11/2002	/	Rusak	Aset Non TI
502	3050201009	Meja Komputer	114	Olympic	11/11/2002	/	Rusak	Aset Non TI
503	3050201009	Meja Komputer	115	Olympic	11/11/2002	/	Rusak	Aset Non TI
504	3050201009	Meja Komputer	116	Olympic	11/11/2002	/	Rusak	Aset Non TI
505	3050201014	Meja Resepsionis	1	Custom	5/29/2017	A05 /	Baik	Aset Non TI
506	3050201014	Meja Resepsionis	2	Custom	5/29/2017	A05 /	Baik	Aset Non TI
507	3050201014	Meja Resepsionis	3	Custom	5/29/2017	A05 /	Baik	Aset Non TI
508	3050201018	Meja Makan Besi	1	Inform	3/22/2017	A04 / R Pelatihan	Baik	Aset Non TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
509	3050201018	Meja Makan Besi	2	Inform	3/22/2017	A04 / R Pelatihan	Baik	Aset Non TI
510	3050201018	Meja Makan Besi	3	Inform	3/22/2017	A04 / R Pelatihan	Baik	Aset Non TI
511	3050201018	Meja Makan Besi	4	Inform	3/22/2017	A04 / R Pelatihan	Baik	Aset Non TI
512	3050201018	Meja Makan Besi	5	Inform	3/22/2017	A04 / R Pelatihan	Baik	Aset Non TI
513	3050201018	Meja Makan Besi	6	Inform	3/22/2017	A04 / R Pelatihan	Baik	Aset Non TI
514	3050201020	Kursi Fiber Glas/Plastik	1	Informa	3/22/2017	A04-1 / R Pelatihan 1	Baik	Aset Non TI
515	3050201020	Kursi Fiber Glas/Plastik	2	Informa	3/22/2017	B02 /	Baik	Aset Non TI
516	3050201020	Kursi Fiber Glas/Plastik	3	Informa	3/22/2017	B02 /	Baik	Aset Non TI
517	3050201020	Kursi Fiber Glas/Plastik	4	Informa	3/22/2017	B02 /	Baik	Aset Non TI
518	3050201020	Kursi Fiber Glas/Plastik	5	Tiger	9/22/2008	/	Baik	Aset Non TI
519	3050201020	Kursi Fiber Glas/Plastik	6	Informa	11/16/2016	A04-2 /	Baik	Aset Non TI
520	3050201020	Kursi Fiber Glas/Plastik	7	Informa	11/16/2016	A04-2 /	Baik	Aset Non TI
521	3050201020	Kursi Fiber Glas/Plastik	8	Informa	11/16/2016	A04-2 /	Baik	Aset Non TI
522	3050201020	Kursi Fiber Glas/Plastik	9	Informa	11/16/2016	A04-2 /	Baik	Aset Non TI
523	3050201020	Kursi Fiber Glas/Plastik	10	Informa	11/16/2016	A04-2 /	Baik	Aset Non TI
524	3050201020	Kursi Fiber Glas/Plastik	11	Informa	11/16/2016	A04-2 /	Baik	Aset Non TI
525	3050201020	Kursi Fiber Glas/Plastik	12	Informa	11/16/2016	/	Baik	Aset Non TI
526	3050201020	Kursi Fiber Glas/Plastik	13	Informa	11/16/2016	A04-3 /	Baik	Aset Non TI
527	3050201020	Kursi Fiber Glas/Plastik	14	Informa	11/16/2016	A04-3 /	Baik	Aset Non TI
528	3050201020	Kursi Fiber Glas/Plastik	15	Informa	11/16/2016	A04-3 /	Baik	Aset Non TI
529	3050201020	Kursi Fiber Glas/Plastik	16	Informa	11/16/2016	A04-3 /	Baik	Aset Non TI
530	3050201020	Kursi Fiber Glas/Plastik	17	Informa	11/16/2016	A04-3 /	Baik	Aset Non TI
531	3050201020	Kursi Fiber Glas/Plastik	18	Informa	11/16/2016	A04-3 /	Baik	Aset Non TI
532	3050201020	Kursi Fiber Glas/Plastik	19	Informa	11/16/2016	A05 /	Baik	Aset Non TI
533	3050201020	Kursi Fiber Glas/Plastik	20	Informa	11/16/2016	A05 /	Baik	Aset Non TI
534	3050201020	Kursi Fiber Glas/Plastik	21	Informa	11/16/2016	A05 /	Baik	Aset Non TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
535	3050201999	Meubelair Lainnya	1	Inform	3/22/2017	A05 /	Baik	Aset Non TI
536	3050201999	Meubelair Lainnya	2	Inform	3/22/2017	A05 /	Baik	Aset Non TI
537	3050203001	Mesin Penghisap Debu/Vacuum Cleaner	1	Nasional	1/1/2004	/	Baik	Aset Non TI
538	3050204001	Lemari Es	1	Panasonic	8/11/2017	A08 /	Baik	Aset Non TI
539	3050204004	A.C. Split	1	Panasonic 2pk	7/14/2015	/	Baik	Aset TI
540	3050204004	A.C. Split	2	Panasonic	9/23/2015	/	Baik	Aset TI
541	3050204004	A.C. Split	8		11/11/2002	/	Rusak	Aset TI
542	3050204004	A.C. Split	19	Panasonik 1,5 PK	5/28/2009	/	Rusak	Aset TI
543	3050204004	A.C. Split	20	LG	8/31/2009	/	Rusak	Aset TI
544	3050204004	A.C. Split	21	Inverter 1 pk	9/22/2010	B02-4 /	Baik	Aset TI
545	3050204004	A.C. Split	22	Type CS-D43DB4H5 (5 HP)	12/6/2010	/	Baik	Aset TI
546	3050204004	A.C. Split	25	AC	12/17/2012	/	Rusak	Aset TI
547	3050204004	A.C. Split	26	AC	12/17/2012	/	Rusak	Aset TI
548	3050204004	A.C. Split	27	Panasonic	12/6/2013	/	Baik	Aset TI
549	3050204004	A.C. Split	28	Panasonic	5/30/2014	/	Baik	Aset TI
550	3050204004	A.C. Split	29	Panasonic	5/30/2014	/	Baik	Aset TI
551	3050204004	A.C. Split	30	Panasonic 2PK	4/19/2016	/	Baik	Aset TI
552	3050204004	A.C. Split	31	Daikin STNE	3/31/2016	VI.3 / Data Center Gd Perpustakaan	Baik	Aset TI
553	3050204004	A.C. Split	32	Daikin STNE	3/31/2016	VI.3 / Data Center Gd Perpustakaan	Baik	Aset TI
554	3050204004	A.C. Split	33	Daikin STNE	3/31/2016	VI.3 / Data Center Gd Perpustakaan	Baik	Aset TI
555	3050204004	A.C. Split	34	Daikin STNE	3/31/2016	VI.3 / Data Center Gd Perpustakaan	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
556	3050204005	Portable Air Conditioner (Alat Pendingin)	1	Panasonic	11/27/2012	/	Rusak	Aset Non TI
557	3050204006	Kipas Angin	5	Panasonic FEP 404	11/7/2017	A04 / R Serbaguna	Baik	Aset Non TI
558	3050204006	Kipas Angin	6	Panasonic FEP 404	11/7/2017	A04-1 / R Pelatihan 1	Baik	Aset Non TI
559	3050204006	Kipas Angin	7	Panasonic FEP 404	11/7/2017	A04-2 / R Pelatihan 2	Baik	Aset Non TI
560	3050204006	Kipas Angin	8	Panasonic FEP 404	11/7/2017	A04-3 / R Pelatihan 3	Baik	Aset Non TI
561	3050204006	Kipas Angin	9	Panasonic FEP 404	11/7/2017	A05 / R Layanan TSI	Baik	Aset Non TI
562	3050204006	Kipas Angin	10	Panasonic FEP 404	11/7/2017	A05 / R Layanan TSI	Baik	Aset Non TI
563	3050204006	Kipas Angin	11	Panasonic FEP 404	11/7/2017	A05-1 / R Kasubdit Yansi	Baik	Aset Non TI
564	3050204006	Kipas Angin	12	Panasonic FEP 404	11/7/2017	A05-2 / R Kasi Ldatin	Baik	Aset Non TI
565	3050204006	Kipas Angin	13	Panasonic FEP 404	11/7/2017	B01 / R Staf IKTI	Baik	Aset Non TI
566	3050204006	Kipas Angin	14	Panasonic FEP 404	11/7/2017	B02 / R Keu & Adm	Baik	Aset Non TI
567	3050204006	Kipas Angin	15	Panasonic FEP 404	11/7/2017	B02-2 / R Staf Bangsi	Baik	Aset Non TI
568	3050204006	Kipas Angin	16	Panasonic FEP 404	11/7/2017	B02-3 / R Rapat Bangsi	Baik	Aset Non TI
569	3050204006	Kipas Angin	17	Panasonic FEP 404	11/7/2017	B02-4 / R Kasubdit Bangsi	Baik	Aset Non TI
570	3050204007	Exhause Fan	1	CKE	8/30/2017	/	Baik	Aset Non TI
571	3050204007	Exhause Fan	2	CKE	8/30/2017	/	Baik	Aset Non TI
572	3050204007	Exhause Fan	3	CKE	8/30/2017	/	Baik	Aset Non TI
573	3050204007	Exhause Fan	4	CKE	8/30/2017	/	Baik	Aset Non TI
574	3050204999	Alat Pendingin Lainnya	1	Panasonic	11/30/2012	/	Rusak	Aset Non TI
575	3050205001	Kompor Listrik (Alat Dapur)	1	Philips	9/26/2018	A08 / R Dapur	Baik	Aset Non TI
576	3050205008	Kitchen Set	1		10/26/2016	A08 / R Dapur	Baik	Aset Non TI
577	3050206002	Televisi	1	Samsung	9/15/2017	A05 / R Layanan TSI	Baik	Aset TI
578	3050206002	Televisi	2	Samsung	9/15/2017	B02 / R Keu & Adm	Baik	Aset TI
579	3050206002	Televisi	3	Panasonic	1/1/2002	/	Baik	Aset TI
580	3050206002	Televisi	7	Sharp	12/4/2014	B01-3 /	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
581	3050206007	Loudspeaker	1	Loudspeaker	12/17/2012	/	Rusak	Aset Non TI
582	3050206007	Loudspeaker	2	Loudspeaker	12/17/2012	/	Rusak	Aset Non TI
583	3050206007	Loudspeaker	3	Rosmaster KD15	12/6/2013	A04 / R Serbaguna	Baik	Aset Non TI
584	3050206012	Wireless	1	cisco	10/21/2010	/ R ME	Rusak	Aset TI
585	3050206012	Wireless	2	cisco	10/21/2010	/ R ME	Rusak	Aset TI
586	3050206012	Wireless	3	cisco	10/21/2010	/ R ME	Rusak	Aset TI
587	3050206012	Wireless	4	cisco	10/21/2010	/ R ME	Rusak	Aset TI
588	3050206012	Wireless	5	cisco	10/21/2010	/ R ME	Rusak	Aset TI
589	3050206012	Wireless	6	cisco	10/21/2010	/ R ME	Rusak	Aset TI
590	3050206012	Wireless	7	cisco	10/21/2010	/ R ME	Rusak	Aset TI
591	3050206012	Wireless	8	cisco	10/21/2010	/ R ME	Rusak	Aset TI
592	3050206012	Wireless	9	cisco	10/21/2010	/ R ME	Rusak	Aset TI
593	3050206012	Wireless	10	cisco	10/21/2010	/ R ME	Rusak	Aset TI
594	3050206012	Wireless	11	cisco	10/21/2010	/ R ME	Rusak	Aset TI
595	3050206012	Wireless	12	cisco	10/21/2010	/ R ME	Rusak	Aset TI
596	3050206012	Wireless	13	cisco	10/21/2010	/ R ME	Rusak	Aset TI
597	3050206012	Wireless	14	cisco	10/21/2010	/ R ME	Rusak	Aset TI
598	3050206012	Wireless	15	cisco	10/21/2010	/ R ME	Rusak	Aset TI
599	3050206012	Wireless	16	cisco	10/21/2010	/ R ME	Rusak	Aset TI
600	3050206012	Wireless	17	cisco	10/21/2010	/ R ME	Rusak	Aset TI
601	3050206012	Wireless	18	cisco	10/21/2010	/ R ME	Rusak	Aset TI
602	3050206012	Wireless	19	cisco	10/21/2010	/ R ME	Rusak	Aset TI
603	3050206012	Wireless	20	cisco	10/21/2010	/ R ME	Rusak	Aset TI
604	3050206012	Wireless	21	cisco	10/21/2010	/ R ME	Rusak	Aset TI
605	3050206012	Wireless	22	cisco	10/21/2010	/ R ME	Rusak	Aset TI
606	3050206012	Wireless	23	cisco	10/21/2010	/ R ME	Rusak	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
607	3050206012	Wireless	24	cisco	10/21/2010	/ R ME	Rusak	Aset TI
608	3050206012	Wireless	25	cisco	10/21/2010	/ R ME	Rusak	Aset TI
609	3050206012	Wireless	26	cisco	10/21/2010	/ R ME	Rusak	Aset TI
610	3050206012	Wireless	27	cisco	10/21/2010	/ R ME	Rusak	Aset TI
611	3050206012	Wireless	28	cisco	10/21/2010	/ R ME	Rusak	Aset TI
612	3050206012	Wireless	29	cisco	10/21/2010	/ R ME	Rusak	Aset TI
613	3050206012	Wireless	30	cisco	10/21/2010	/ R ME	Rusak	Aset TI
614	3050206012	Wireless	31	cisco	10/21/2010	/ R ME	Rusak	Aset TI
615	3050206012	Wireless	32	cisco	10/21/2010	/ R ME	Rusak	Aset TI
616	3050206012	Wireless	33	cisco	10/21/2010	/ R ME	Rusak	Aset TI
617	3050206012	Wireless	34	cisco	10/21/2010	/ R ME	Rusak	Aset TI
618	3050206012	Wireless	35	cisco	10/21/2010	/ R ME	Rusak	Aset TI
619	3050206012	Wireless	36	cisco	10/21/2010	/ R ME	Rusak	Aset TI
620	3050206012	Wireless	37	cisco	10/21/2010	/ R ME	Rusak	Aset TI
621	3050206012	Wireless	38	cisco	10/21/2010	/ R ME	Rusak	Aset TI
622	3050206012	Wireless	39	cisco	10/21/2010	/ R ME	Rusak	Aset TI
623	3050206012	Wireless	40	cisco	10/21/2010	/ R ME	Rusak	Aset TI
624	3050206012	Wireless	41	cisco	10/21/2010	/ R ME	Rusak	Aset TI
625	3050206012	Wireless	42	cisco	10/21/2010	/ R ME	Rusak	Aset TI
626	3050206012	Wireless	43	cisco	10/21/2010	/ R ME	Rusak	Aset TI
627	3050206012	Wireless	44	cisco	10/21/2010	/ R ME	Rusak	Aset TI
628	3050206012	Wireless	45	cisco	10/21/2010	/ R ME	Rusak	Aset TI
629	3050206012	Wireless	46	cisco	10/21/2010	/ R ME	Rusak	Aset TI
630	3050206012	Wireless	47	cisco	10/21/2010	/ R ME	Rusak	Aset TI
631	3050206012	Wireless	48	cisco	10/21/2010	/ R ME	Rusak	Aset TI
632	3050206012	Wireless	49	cisco	10/21/2010	/ R ME	Rusak	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
633	3050206012	Wireless	50	cisco	10/21/2010	/ R ME	Rusak	Aset TI
634	3050206012	Wireless	51	cisco	10/21/2010	/ R ME	Rusak	Aset TI
635	3050206012	Wireless	52	cisco	10/21/2010	/ R ME	Rusak	Aset TI
636	3050206012	Wireless	53	cisco	10/21/2010	/ R ME	Rusak	Aset TI
637	3050206012	Wireless	54	cisco	10/21/2010	/ R ME	Rusak	Aset TI
638	3050206012	Wireless	55	cisco	10/21/2010	/ R ME	Rusak	Aset TI
639	3050206012	Wireless	56	cisco	10/21/2010	/ R ME	Rusak	Aset TI
640	3050206012	Wireless	57	cisco	10/21/2010	/ R ME	Rusak	Aset TI
641	3050206012	Wireless	58	cisco	10/21/2010	/ R ME	Rusak	Aset TI
642	3050206012	Wireless	59	cisco	10/21/2010	/ R ME	Rusak	Aset TI
643	3050206012	Wireless	60	cisco	10/21/2010	/ R ME	Rusak	Aset TI
644	3050206012	Wireless	61	cisco	10/21/2010	/ R ME	Rusak	Aset TI
645	3050206012	Wireless	62	cisco	10/21/2010	/ R ME	Rusak	Aset TI
646	3050206012	Wireless	63	cisco	10/21/2010	/ R ME	Rusak	Aset TI
647	3050206012	Wireless	64	cisco	10/21/2010	/ R ME	Rusak	Aset TI
648	3050206012	Wireless	65	cisco	10/21/2010	/ R ME	Rusak	Aset TI
649	3050206012	Wireless	66	cisco	10/21/2010	/ R ME	Rusak	Aset TI
650	3050206012	Wireless	67	cisco	10/21/2010	/ R ME	Rusak	Aset TI
651	3050206012	Wireless	68	cisco	10/21/2010	/ R ME	Rusak	Aset TI
652	3050206012	Wireless	69	cisco	10/21/2010	/ R ME	Rusak	Aset TI
653	3050206012	Wireless	70	cisco	10/21/2010	/ R ME	Rusak	Aset TI
654	3050206012	Wireless	71	cisco	10/21/2010	/ R ME	Rusak	Aset TI
655	3050206012	Wireless	72	cisco	10/21/2010	/ R ME	Rusak	Aset TI
656	3050206012	Wireless	73	cisco	10/21/2010	/ R ME	Rusak	Aset TI
657	3050206012	Wireless	74	cisco	10/21/2010	/ R ME	Rusak	Aset TI
658	3050206012	Wireless	75	cisco	10/21/2010	/ R ME	Rusak	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
659	3050206012	Wireless	76	cisco	10/21/2010	/ R ME	Rusak	Aset TI
660	3050206012	Wireless	77	cisco	10/21/2010	/ R ME	Rusak	Aset TI
661	3050206012	Wireless	78	cisco	10/21/2010	/ R ME	Rusak	Aset TI
662	3050206012	Wireless	79	cisco	10/21/2010	/ R ME	Rusak	Aset TI
663	3050206012	Wireless	80	cisco	10/21/2010	/ R ME	Rusak	Aset TI
664	3050206012	Wireless	81	cisco	10/21/2010	/ R ME	Rusak	Aset TI
665	3050206012	Wireless	82	cisco	10/21/2010	/ R ME	Rusak	Aset TI
666	3050206012	Wireless	83	cisco	10/21/2010	/ R ME	Rusak	Aset TI
667	3050206012	Wireless	84	cisco	10/21/2010	/ R ME	Rusak	Aset TI
668	3050206012	Wireless	85	cisco	10/21/2010	/ R ME	Rusak	Aset TI
669	3050206012	Wireless	86	cisco	10/21/2010	/ R ME	Rusak	Aset TI
670	3050206012	Wireless	87	cisco	10/21/2010	/ R ME	Rusak	Aset TI
671	3050206012	Wireless	88	cisco	10/21/2010	/ R ME	Rusak	Aset TI
672	3050206012	Wireless	89	cisco	10/21/2010	/ R ME	Rusak	Aset TI
673	3050206012	Wireless	90	cisco	10/21/2010	/ R ME	Rusak	Aset TI
674	3050206012	Wireless	91	cisco	10/21/2010	/ R ME	Rusak	Aset TI
675	3050206012	Wireless	92	cisco	10/21/2010	/ R ME	Rusak	Aset TI
676	3050206012	Wireless	93	cisco	10/21/2010	/ R ME	Rusak	Aset TI
677	3050206012	Wireless	94	cisco	10/21/2010	/ R ME	Rusak	Aset TI
678	3050206012	Wireless	95	cisco	10/21/2010	/ R ME	Rusak	Aset TI
679	3050206012	Wireless	96	cisco	10/21/2010	/ R ME	Rusak	Aset TI
680	3050206012	Wireless	97	cisco	10/21/2010	/ R ME	Rusak	Aset TI
681	3050206012	Wireless	98	cisco	10/21/2010	/ R ME	Rusak	Aset TI
682	3050206012	Wireless	99	cisco	10/21/2010	/ R ME	Rusak	Aset TI
683	3050206012	Wireless	100	cisco	10/21/2010	/ R ME	Rusak	Aset TI
684	3050206015	Microphone Table Stand	1	Desk Microphone	12/17/2012	/	Rusak	Aset Non TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
685	3050206015	Microphone Table Stand	2	Desk Microphone	12/17/2012	/	Rusak	Aset Non TI
686	3050206015	Microphone Table Stand	3	Desk Microphone	12/17/2012	/	Rusak	Aset Non TI
687	3050206015	Microphone Table Stand	4	Desk Microphone	12/17/2012	/	Rusak	Aset Non TI
688	3050206015	Microphone Table Stand	5	Desk Microphone	12/17/2012	/	Rusak	Aset Non TI
689	3050206015	Microphone Table Stand	6	Desk Microphone	12/17/2012	/	Rusak	Aset Non TI
690	3050206017	Unit Power Supply	2	Sendon SUPS 1525	11/11/2002	B00 / Selasar Selatan	Rusak	Aset TI
691	3050206017	Unit Power Supply	4	sendon SUPS 1525	11/11/2002	B00 / Selasar Selatan	Rusak	Aset TI
692	3050206017	Unit Power Supply	5	Sendon SUPS 1525	11/11/2002	B00 / Selasar Selatan	Rusak	Aset TI
693	3050206017	Unit Power Supply	7	APC Smart	1/1/2003	/	Baik	Aset TI
694	3050206020	Camera Video	1	HD Additional Camera	12/17/2012	/	Rusak	Aset TI
695	3050206020	Camera Video	2	Document Camera	12/17/2012	/	Rusak	Aset TI
696	3050206034	Tangga Aluminium	1		11/11/2002	A06 / R ME	Baik	Aset Non TI
697	3050206036	Dispenser	3	Sharp SWD75EHLBD	12/6/2013	B02-2 /	Baik	Aset Non TI
698	3050206036	Dispenser	4	Sharp SWD75EHLBD	12/6/2013	/	Baik	Aset Non TI
699	3050206036	Dispenser	5	Sanken/HWD-Z88	11/23/2017		Baik	Aset Non TI
700	3050206036	Dispenser	6	Sanken	12/15/2017	A04 /	Rusak	Aset Non TI
701	3050206045	Coffee Maker	1	Elektrolux	1/1/2004	A06 / R ME	Rusak	Aset Non TI
702	3050206046	Handy Cam	1	Sony	12/4/2013	A05 / R Layanan TSI	Baik	Aset Non TI
703	3050206073	Jemuran	1	Krisbow	9/21/2018	A09 / K Mandi	Baik	Aset Non TI
704	3050206080	Bracket Standing Peralatan	1	Untuk LCD 40	12/11/2014	B01-3 / B02-3	Baik	Aset Non TI
705	3050206999	Alat Rumah Tangga Lainnya (Home Use)	1	Visual Fault Locator/ Senter FO	6/30/2014	B01 / R. IKTI	Baik	Aset Non TI
706	3060101036	Microphone/Wireless MIC	1	Wireless Microphone	12/17/2012	/	Rusak	Aset Non TI
707	3060101036	Microphone/Wireless MIC	2	Wireless Microphone	12/17/2012	/	Rusak	Aset Non TI
708	3060101048	Uninterruptible Power Supply (UPS)	1	APC BRI 100CI-AS	5/3/2010	/	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
709	3060101048	Uninterruptible Power Supply (UPS)	2	APC BRI 100CI-AS	5/3/2010	/	Baik	Aset TI
710	3060101048	Uninterruptible Power Supply (UPS)	3	UPS ONLINE	10/21/2010	/	Baik	Aset TI
711	3060101048	Uninterruptible Power Supply (UPS)	4	UPS ONLINE	10/21/2010	/	Baik	Aset TI
712	3060101048	Uninterruptible Power Supply (UPS)	5	UPS ONLINE	10/21/2010	/	Baik	Aset TI
713	3060101048	Uninterruptible Power Supply (UPS)	6	UPS ONLINE	10/21/2010	/	Baik	Aset TI
714	3060101048	Uninterruptible Power Supply (UPS)	7	UPS ONLINE	10/21/2010	/	Baik	Aset TI
715	3060101048	Uninterruptible Power Supply (UPS)	8	UPS ONLINE	10/21/2010	/	Baik	Aset TI
716	3060101048	Uninterruptible Power Supply (UPS)	9	UPS ONLINE	10/21/2010	/	Baik	Aset TI
717	3060101048	Uninterruptible Power Supply (UPS)	10	UPS	12/17/2012	/	Baik	Aset TI
718	3060101048	Uninterruptible Power Supply (UPS)	11	ICA	12/3/2013	/	Rusak	Aset TI
719	3060101048	Uninterruptible Power Supply (UPS)	12	PASCAL Modular RM	10/1/2014	/	Baik	Aset TI
720	3060101048	Uninterruptible Power Supply (UPS)	13	APC Smart UPS C1000	12/12/2017	B02-2 /	Baik	Aset TI
721	3060101048	Uninterruptible Power Supply (UPS)	14	APC Smart UPS C1000	12/12/2017	B02-2 /	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
722	3060101048	Uninterruptible Power Supply (UPS)	15	APC Smart UPS C1000	12/12/2017	B02-2 /	Baik	Aset TI
723	3060101048	Uninterruptible Power Supply (UPS)	16	APC Smart UPS C1000	12/12/2017	B02-2 /	Baik	Aset TI
724	3060101048	Uninterruptible Power Supply (UPS)	17	APC Smart UPS C1000	12/12/2017	B02-2 /	Baik	Aset TI
725	3060101048	Uninterruptible Power Supply (UPS)	18	APC Smart UPS C1000	12/12/2017	B02-2 /	Baik	Aset TI
726	3060101048	Uninterruptible Power Supply (UPS)	19	APC Smart UPS C1000	12/12/2017	B02-2 /	Baik	Aset TI
727	3060101048	Uninterruptible Power Supply (UPS)	20	APC Smart UPS C1000	12/12/2017	B02-2 /	Baik	Aset TI
728	3060101048	Uninterruptible Power Supply (UPS)	21	APC Smart UPS C1000	12/12/2017	B02-3 /	Baik	Aset TI
729	3060101048	Uninterruptible Power Supply (UPS)	22	APC Smart UPS C1000	12/12/2017	B02 /	Baik	Aset TI
730	3060101048	Uninterruptible Power Supply (UPS)	23	APC Smart UPS C1000	12/12/2017	A05 /	Baik	Aset TI
731	3060101048	Uninterruptible Power Supply (UPS)	24	APC	12/26/2018	/	Baik	Aset TI
732	3060101048	Uninterruptible Power Supply (UPS)	25	APC	12/26/2018	/	Baik	Aset TI
733	3060101048	Uninterruptible Power Supply (UPS)	26	APC	12/26/2018	/	Baik	Aset TI
734	3060101048	Uninterruptible Power Supply (UPS)	27	APC	12/26/2018	/	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
735	3060101048	Uninterruptible Power Supply (UPS)	28	APC	12/26/2018	/	Baik	Aset TI
736	3060101048	Uninterruptible Power Supply (UPS)	29	APC	12/26/2018	/	Baik	Aset TI
737	3060101048	Uninterruptible Power Supply (UPS)	30	APC	12/26/2018	/	Baik	Aset TI
738	3060101048	Uninterruptible Power Supply (UPS)	31	APC	12/26/2018	A04-2 / R Pelatihan 2	Baik	Aset TI
739	3060101048	Uninterruptible Power Supply (UPS)	32	APC	12/26/2018	A04-2 / R Pelatihan 2	Baik	Aset TI
740	3060101048	Uninterruptible Power Supply (UPS)	33	APC	12/26/2018	A04-2 / R Pelatihan 2	Baik	Aset TI
741	3060101048	Uninterruptible Power Supply (UPS)	34	APC	12/26/2018	A04-2 / R Pelatihan 2	Baik	Aset TI
742	3060101048	Uninterruptible Power Supply (UPS)	35	APC	12/26/2018	A04-2 / R Pelatihan 2	Baik	Aset TI
743	3060101048	Uninterruptible Power Supply (UPS)	36	APC	12/26/2018	A04-2 / R Pelatihan 2	Baik	Aset TI
744	3060101048	Uninterruptible Power Supply (UPS)	37	APC	12/26/2018	A04-3 / R Pelatihan 3	Baik	Aset TI
745	3060101048	Uninterruptible Power Supply (UPS)	38	APC	12/26/2018	A04-3 / R Pelatihan 3	Baik	Aset TI
746	3060101048	Uninterruptible Power Supply (UPS)	39	APC	12/26/2018	A04-3 / R Pelatihan 3	Baik	Aset TI
747	3060101048	Uninterruptible Power Supply (UPS)	40	APC	12/26/2018	A04-3 / R Pelatihan 3	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
748	3060101048	Uninterruptible Power Supply (UPS)	41	APC	12/26/2018	A04-3 / R Pelatihan 3	Baik	Aset TI
749	3060101048	Uninterruptible Power Supply (UPS)	42	APC	12/26/2018	A04-3 / R Pelatihan 3	Baik	Aset TI
750	3060101048	Uninterruptible Power Supply (UPS)	43	APC	12/26/2018	A05 / R Layanan TSI	Baik	Aset TI
751	3060101048	Uninterruptible Power Supply (UPS)	44	APC	12/26/2018	A05 / R Layanan TSI	Baik	Aset TI
752	3060101048	Uninterruptible Power Supply (UPS)	45	APC	12/26/2018	A05 / R Layanan TSI	Baik	Aset TI
753	3060101048	Uninterruptible Power Supply (UPS)	46	APC	12/26/2018	A05 / R Layanan TSI	Baik	Aset TI
754	3060101048	Uninterruptible Power Supply (UPS)	47	APC	12/26/2018	A05 / R Layanan TSI	Baik	Aset TI
755	3060101048	Uninterruptible Power Supply (UPS)	48	APC	12/26/2018	A05 / R Layanan TSI	Baik	Aset TI
756	3060101048	Uninterruptible Power Supply (UPS)	49	APC	12/26/2018	A05-2 / R Kasubdit Yansi	Baik	Aset TI
757	3060101048	Uninterruptible Power Supply (UPS)	50	APC	12/26/2018	A05-3 / R Kasi Ldatin	Baik	Aset TI
758	3060101048	Uninterruptible Power Supply (UPS)	51	APC	12/26/2018	B01-4 / R Kasubdit IKTI	Baik	Aset TI
759	3060101048	Uninterruptible Power Supply (UPS)	52	APC	12/26/2018	B02 / R Keu & Adm	Baik	Aset TI
760	3060101048	Uninterruptible Power Supply (UPS)	53	APC	12/26/2018	B02-2 / R Staf Bangsi	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
761	3060101048	Uninterruptible Power Supply (UPS)	54	APC	12/26/2018	B02-3 / R Rapat Bangsi	Baik	Aset TI
762	3060101048	Uninterruptible Power Supply (UPS)	55	APC	12/26/2018	B02-3 / R Rapat Bangsi	Baik	Aset TI
763	3060101048	Uninterruptible Power Supply (UPS)	56	APC	12/26/2018	B02-4 / R Kasubdit Yansi	Baik	Aset TI
764	3060101048	Uninterruptible Power Supply (UPS)	57	APC	12/26/2018	B02-4 / R Kasubdit Yansi	Baik	Aset TI
765	3060101048	Uninterruptible Power Supply (UPS)	58	APC	12/26/2018	/	Baik	Aset TI
766	3060101048	Uninterruptible Power Supply (UPS)	59	APC	12/26/2018	/	Baik	Aset TI
767	3060101048	Uninterruptible Power Supply (UPS)	60	APC	12/26/2018	/	Baik	Aset TI
768	3060101048	Uninterruptible Power Supply (UPS)	61	APC	12/26/2018	/	Baik	Aset TI
769	3060101056	Battery Charger (Peralatan Studio Audio)	1	Pascal	11/28/2014	B01 / R Staf IKTI	Baik	Aset Non TI
770	3060101060	Power Amplifier	1	Power Amplifier	12/17/2012	/	Rusak	Aset Non TI
771	3060101065	Chairman/Audio Conference	1	Audio Conference System	12/17/2012	/	Rusak	Aset Non TI
772	3060101076	Digital Audio Taperecorder	1	Voice Recorder Sony ICD-PX440/C	12/31/2017	/	Rusak	Aset Non TI
773	3060101085	Cable	1	Kabel video conference	12/17/2012	/	Rusak	Aset Non TI
774	3060102012	Video Monitor	1	Lecturer Monitor	12/17/2012	/	Rusak	Aset Non TI
775	3060102013	Video Tape Recorder Portable	1	Video Recorder	12/17/2012	/	Rusak	Aset Non TI
776	3060102015	Video Mixer	1	Video Mixer	12/17/2012	/	Rusak	Aset Non TI
777	3060102045	Tripod Camera	1	Fotopro 9300	11/14/2017	B01-2 / R. Rapat IKTI	Baik	Aset Non TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
778	3060102045	Tripod Camera	2	Fotopro 9300	11/14/2017	B01-2 / R. Rapat IKTI	Baik	Aset Non TI
779	3060102128	Camera Digital	1	Canon EOS 70D 18-135 mm f/3.5	12/31/2017	B03-1 / R Sekretariat SBMPTN	Baik	Aset Non TI
780	3060102132	Video Conference	1	Video Conference Codec	12/17/2012	/	Rusak	Aset Non TI
781	3060102135	LCD Monitor	1	LCD Video Monitor	12/17/2012	/	Baik	Aset TI
782	3060102135	LCD Monitor	2	Samsung 32"	12/6/2013	A05 /	Baik	Aset TI
783	3060102135	LCD Monitor	3	Samsung 32"	12/6/2013	A05 /	Baik	Aset TI
784	3060102135	LCD Monitor	4	LG	12/14/2018	B02-2 /	Baik	Aset TI
785	3060102135	LCD Monitor	5	LG	12/14/2018	B02-2 /	Baik	Aset TI
786	3060102135	LCD Monitor	6	LG	12/14/2018	B02-2 /	Baik	Aset TI
787	3060102135	LCD Monitor	7	LG	12/14/2018	B02-2 /	Baik	Aset TI
788	3060102135	LCD Monitor	8	LG	12/14/2018	A05 /	Baik	Aset TI
789	3060102165	Camera Conference	1	Logitech	12/21/2018	B01-3 / R Rapat IKTI	Baik	Aset TI
790	3060102165	Camera Conference	2	Logitech	12/21/2018	B01-3 / R Rapat IKTI	Baik	Aset TI
791	3060201001	Telephone (PABX)	1	Panasonic	11/26/2015	/	Baik	Aset TI
792	3060201001	Telephone (PABX)	9	Panasonic KX-NS300	5/19/2016	/	Baik	Aset TI
793	3060201003	Pesawat Telephone	1	Panasonic KWI 505	12/9/2013	B02 / R Keu & Adm	Baik	Aset TI
794	3060201003	Pesawat Telephone	2	Panasonic KWI 505	12/9/2013	B02 / R Keu & Adm	Baik	Aset TI
795	3060201004	Telephone Mobile	1	Samsung	12/15/2017	B02-2 / R Staf Pusbang	Baik	Aset TI
796	3060201004	Telephone Mobile	2	Samsung S8+	12/15/2017	B02-2 / R Staf Pusbang	Baik	Aset TI
797	3060201004	Telephone Mobile	3	Apple iPhone 7 Plus	12/15/2017	B02-2 / R Staf Pusbang	Baik	Aset TI
798	3060201004	Telephone Mobile	4	Apple iPhone 7 JetBlack	12/15/2017	B02-2 / R Staf Pusbang	Baik	Aset TI
799	3060201006	Handy Talky (HT)	3	Icom V80	6/27/2011	B01-3 / R Rapat IKTI	Baik	Aset Non TI
800	3060201006	Handy Talky (HT)	4	Icom V80	6/27/2011	B01-3 / R Rapat IKTI	Baik	Aset Non TI
801	3060201006	Handy Talky (HT)	5	Taffware Walkie Talkie Dual Band 5W	12/31/2017	/	Rusak	Aset Non TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
802	3060201006	Handy Talky (HT)	6	Taffware Walkie Talkie Dual Band 5W	12/31/2017	/	Rusak	Aset Non TI
803	3060201006	Handy Talky (HT)	7	Taffware Walkie Talkie Dual Band 5W	12/31/2017	/	Rusak	Aset Non TI
804	3060201006	Handy Talky (HT)	8	Taffware Walkie Talkie Dual Band 5W	12/31/2017	/	Rusak	Aset Non TI
805	3060323015	Switcher/Patch Panel	1	Switch	8/31/2009	B02-2 /	Baik	Aset TI
806	3060347002	Genset	1	CATERPILLAR ECW00427	12/17/2015	LL / Lt Dasar RC	Baik	Aset TI
807	3070106082	Modulas Monitoring System	1	Modul	8/31/2009	/	Baik	Aset TI
808	3070107063	Fiber Optic Operating	1	GE	8/21/2010	/	Baik	Aset TI
809	3080111023	Timbangan/Neraca	1	Tanika	11/11/2002	A10 / Gd ATK	Baik	Aset Non TI
810	3080111174	Digital Indicator LCD/Metric	1	Display key telp.	10/8/2010	A05 / R Pusyan	Baik	Aset TI
811	3080141194	Personal Computer	1	HP	12/12/2012	/	Baik	Aset TI
812	3080141251	Stabilizer/UPS	1	UPS Protekta	8/31/2009	VI.3 / Data Center Gd Perpustakaan	Baik	Aset TI
813	3080161012	Instalasi Fiber Optic LCD Projector Multimedia	1	CISCO	8/21/2010	/	Rusak	Aset TI
814	3080161012	Instalasi Fiber Optic LCD Projector Multimedia	2	CISCO	10/21/2010	/	Rusak	Aset TI
815	3080203117	Panel Uto Power	1	Panel Listrik	8/31/2009	/	Baik	Aset TI
816	3080205001	Generator Set (Lab Scale)	1	Genset & ATS	8/31/2009	UPT Fasor / Samping Gd Badminton	Rusak	Aset TI
817	3080305002	Uninterupted Power Supply (UPS)	1	PROLINK PRO 930 3000VA	12/30/2010	/	Baik	Aset TI
818	3080305002	Uninterupted Power Supply (UPS)	2	PROLINK PRO 930 3000VA	12/30/2010	/	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
819	3080305002	Uninterupted Power Supply (UPS)	3	UPS ICA RN 3200C	6/27/2011	/	Baik	Aset TI
820	3080305002	Uninterupted Power Supply (UPS)	4	UPS ICA RN 3200C	6/27/2011	/	Baik	Aset TI
821	3080305002	Uninterupted Power Supply (UPS)	5	UPS ICA RN 3200C	6/27/2011	/	Baik	Aset TI
822	3080305002	Uninterupted Power Supply (UPS)	6	UPS ICA RN 3200C	6/27/2011	/	Baik	Aset TI
823	3080305002	Uninterupted Power Supply (UPS)	7	Rackmounted TCL3300	11/12/2012	VI.3 / Data Center Gd Perpustakaan	Baik	Aset TI
824	3080305002	Uninterupted Power Supply (UPS)	8	APC/UPS Smart	7/18/2013	/	Baik	Aset TI
825	3080305002	Uninterupted Power Supply (UPS)	9	APC/UPS Smart	7/18/2013	/	Baik	Aset TI
826	3080305002	Uninterupted Power Supply (UPS)	10	ICA 1231C	12/6/2013	/	Rusak	Aset TI
827	3080703004	Software DAAS MOD	1	Software Pengemb. Sistem Infor Manj (CMMS)	12/30/2010	/	Baik	Aset TI
828	3080714009	Interface	1	CISCO	10/21/2010	/	Baik	Aset TI
829	3080806025	Paralel Control Network	1	CISCO	10/21/2010	/	Baik	Aset TI
830	3100101004	Internet	1	CISCO	10/21/2010	/	Baik	Aset TI
831	3100101999	Komputer Jaringan Lainnya	1	HP	12/11/2012	/	Baik	Aset TI
832	3100102001	P.C Unit	1	Intel NUC	9/4/2017	A04-2 / R Pelatihan 2	Baik	Aset TI
833	3100102001	P.C Unit	2	Intel NUC	9/4/2017	A04-2 / R Pelatihan 2	Baik	Aset TI
834	3100102001	P.C Unit	3	Intel NUC	9/4/2017	A04-2 / R Pelatihan 2	Baik	Aset TI
835	3100102001	P.C Unit	4	Intel NUC	9/4/2017	A04-2 / R Pelatihan 2	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
836	3100102001	P.C Unit	5	Intel NUC	9/4/2017	A04-2 / R Pelatihan 2	Baik	Aset TI
837	3100102001	P.C Unit	6	Intel NUC	9/4/2017	A04-2 / R Pelatihan 2	Baik	Aset TI
838	3100102001	P.C Unit	7	Intel NUC	9/4/2017	A04-3 / R Pelatihan 3	Baik	Aset TI
839	3100102001	P.C Unit	8	Intel NUC	9/4/2017	A04-3 / R Pelatihan 3	Baik	Aset TI
840	3100102001	P.C Unit	9	Intel NUC	9/4/2017	A04-3 / R Pelatihan 3	Baik	Aset TI
841	3100102001	P.C Unit	10	Intel NUC	9/4/2017	A04-3 / R Pelatihan 3	Baik	Aset TI
842	3100102001	P.C Unit	11	Intel NUC	9/4/2017	A04-3 / R Pelatihan 3	Baik	Aset TI
843	3100102001	P.C Unit	12	Intel NUC	9/4/2017	A04-3 / R Pelatihan 3	Baik	Aset TI
844	3100102001	P.C Unit	13	HP/Slimline	11/20/2015	B02-2 / R Staf Bangsi	Baik	Aset TI
845	3100102001	P.C Unit	21	HP Omni 200-5316L	6/30/2011	B02 / R Keu & Adm	Baik	Aset TI
846	3100102001	P.C Unit	22	HP Pavilion	12/5/2013	/	Baik	Aset TI
847	3100102001	P.C Unit	23	HP Pavilion	12/5/2013	/	Baik	Aset TI
848	3100102001	P.C Unit	24	Simbadda	9/16/2014	/	Baik	Aset TI
849	3100102001	P.C Unit	25	Simbadda	9/16/2014	/	Baik	Aset TI
850	3100102001	P.C Unit	26	Simbadda	9/16/2014	/	Baik	Aset TI
851	3100102001	P.C Unit	27	HP Pro 4300SFF	12/10/2014	/	Baik	Aset TI
852	3100102001	P.C Unit	28	HP Pro 4300SFF	12/10/2014	/	Baik	Aset TI
853	3100102001	P.C Unit	29	hp	7/28/2016	A04-1 /	Baik	Aset TI
854	3100102001	P.C Unit	30	hp	7/28/2016	A04-1 /	Baik	Aset TI
855	3100102001	P.C Unit	31	hp	7/28/2016	A04-1 /	Baik	Aset TI
856	3100102001	P.C Unit	32	HP Pavilion 24-B121D	12/31/2017	/	Baik	Aset TI
857	3100102002	Lap Top	1	Thosiba Satelite	11/11/2002	B02-2 /	Rusak	Aset TI
858	3100102002	Lap Top	2	IBM	1/1/2003	B02-2 /	Rusak	Aset TI
859	3100102002	Lap Top	3	TOSHIBA	1/1/2004	B02-2 /	Rusak	Aset TI
860	3100102002	Lap Top	4	Toshiba	1/6/2004	B02-2 /	Rusak	Aset TI
861	3100102002	Lap Top	5	Mac Book Pro MC374 13"	12/8/2010	A05 / R Layanan TSI	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
862	3100102002	Lap Top	6	Asus ZenBook Flip UX360CA-C4115T	12/31/2017	B02-2 / R Staf Bangsi	Baik	Aset TI
863	3100102002	Lap Top	7	NoteBook Asus ZenBookAsus UX390UA-GS048T	12/31/2017	B02-2 / R Staf Bangsi	Baik	Aset TI
864	3100102002	Lap Top	8	Apple Macbook MNYG2ID/A	12/31/2017	/	Baik	Aset TI
865	3100102003	Note Book	1	HP Mini	8/25/2011	B01 / R Staf IKTI	Baik	Aset TI
866	3100102003	Note Book	2	HP Probook 4330s	6/27/2011	B02-2 / R Staf IKTI	Baik	Aset TI
867	3100102003	Note Book	3	HP Probook 4330s	6/27/2011	B02-2 /	Baik	Aset TI
868	3100102003	Note Book	4	HP Probook 4330s	6/27/2011	B02-2 /	Baik	Aset TI
869	3100102003	Note Book	5	HP probook	8/31/2012	B01 / R Staf IKTI	Baik	Aset TI
870	3100102003	Note Book	6	HP	12/11/2012	B02-2 /	Baik	Aset TI
871	3100102003	Note Book	7	HP	12/11/2012	B02-2 /	Baik	Aset TI
872	3100102003	Note Book	8	Lenovo	12/12/2012	B02 /	Baik	Aset TI
873	3100102003	Note Book	9	HP	12/12/2012	B02-2 /	Baik	Aset TI
874	3100102003	Note Book	10	Sony	12/4/2013	B01 / R. IKTI	Baik	Aset TI
875	3100102003	Note Book	11	Lenovo	12/12/2013	A05 /	Baik	Aset TI
876	3100102003	Note Book	12	Lenovo	12/12/2013	B01 / R Staf IKTI	Baik	Aset TI
877	3100102003	Note Book	13	HP/430	9/30/2014	B02-2 /	Baik	Aset TI
878	3100102003	Note Book	14	Lenovo/G40	9/30/2014	A05 /	Baik	Aset TI
879	3100102003	Note Book	15	Lenovo/G40	9/30/2014	B02-2 /	Baik	Aset TI
880	3100102003	Note Book	16	Apple	10/30/2017	B02-2 /	Baik	Aset TI
881	3100102003	Note Book	17	Lenovo	10/31/2017	A05 /	Baik	Aset TI
882	3100102003	Note Book	18	Lenovo	10/31/2017	A05 /	Baik	Aset TI
883	3100102003	Note Book	19	Asus A45 6UR putih	11/29/2017	A05 /	Baik	Aset TI
884	3100102003	Note Book	20	Asus A45 6UR putih	11/29/2017	A05 /	Baik	Aset TI
885	3100102003	Note Book	21	Asus A45 6UR putih	11/29/2017	A05 /	Baik	Aset TI
886	3100102003	Note Book	22	Asus A45 6UR putih	11/29/2017	A05 /	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
887	3100102003	Note Book	23	Asus	12/6/2017	A05 /	Baik	Aset TI
888	3100102003	Note Book	24	Asus	12/6/2017	A05 /	Baik	Aset TI
889	3100102003	Note Book	25	Asus	12/6/2017	A05 /	Baik	Aset TI
890	3100102003	Note Book	26	DELL Inspiron 14 (7460)	12/21/2017	B01 / R. IKTI	Baik	Aset TI
891	3100102003	Note Book	27	DELL Inspiron 14 (7460)	12/21/2017	B01 / R. IKTI	Baik	Aset TI
892	3100102008	Ultra Mobile P.C.	1	Apple iPad Wi-Fi	12/15/2017	B02-2 / R Staf Pusbang	Baik	Aset TI
893	3100102008	Ultra Mobile P.C.	2	Samsung Tab3	12/15/2017	B02-2 / R Staf Pusbang	Baik	Aset TI
894	3100102999	Personal Komputer Lainnya	1	-	12/11/2012	B02-2 / R Staf Pusbang	Baik	Aset TI
895	3100102999	Personal Komputer Lainnya	2	-	12/11/2012	B02-2 / R Staf Pusbang	Baik	Aset TI
896	3100102999	Personal Komputer Lainnya	3	-	12/11/2012	B02-2 / R Staf Pusbang	Baik	Aset TI
897	3100102999	Personal Komputer Lainnya	4	-	12/11/2012	B02-2 / R Staf Pusbang	Baik	Aset TI
898	3100201004	Storage Modul Disk (Peralatan Mainframe)	1	SAN/Storage	7/18/2012	/	Baik	Aset TI
899	3100201004	Storage Modul Disk (Peralatan Mainframe)	2	Hitachi/HUS110	12/10/2014	B01-2 /	Baik	Aset TI
900	3100202010	Scanner (Peralatan Mini Komputer)	1	NCS OPSCAN 5	11/11/2002	B03-2 / R Proses Data	Baik	Aset TI
901	3100202010	Scanner (Peralatan Mini Komputer)	2	NCS OPSCAN 5	11/11/2002	B03-2 / R Proses Data	Baik	Aset TI
902	3100202010	Scanner (Peralatan Mini Komputer)	3	NCS OPSCAN 5	11/11/2002	B03-2 / R Proses Data	Baik	Aset TI
903	3100202010	Scanner (Peralatan Mini Komputer)	4	NCS OPSCAN 5	11/11/2002	B03-2 / R Proses Data	Baik	Aset TI
904	3100202010	Scanner (Peralatan Mini Komputer)	5	NCS OPSCAN 5	11/11/2002	B03-2 / R Proses Data	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
905	3100202010	Scanner (Peralatan Mini Komputer)	6	canon	1/1/2004	/	Baik	Aset TI
906	3100202010	Scanner (Peralatan Mini Komputer)	7	Intermec/SG20	9/16/2014	B01-3 / R Rapat IKTI	Baik	Aset TI
907	3100202015	Auto Switch/Data Switch	1	CISCO	10/21/2010	/	Baik	Aset TI
908	3100202015	Auto Switch/Data Switch	2	CISCO	10/21/2010	/	Baik	Aset TI
909	3100202015	Auto Switch/Data Switch	3	CISCO	10/21/2010	/	Baik	Aset TI
910	3100202015	Auto Switch/Data Switch	4	CISCO	10/21/2010	/	Baik	Aset TI
911	3100202015	Auto Switch/Data Switch	5	CISCO	10/21/2010	/	Baik	Aset TI
912	3100202015	Auto Switch/Data Switch	6	CISCO	10/21/2010	/	Baik	Aset TI
913	3100202015	Auto Switch/Data Switch	7	CISCO	10/21/2010	/	Baik	Aset TI
914	3100202015	Auto Switch/Data Switch	8	CISCO	10/21/2010	/	Baik	Aset TI
915	3100202015	Auto Switch/Data Switch	9	CISCO	10/21/2010	/	Baik	Aset TI
916	3100202015	Auto Switch/Data Switch	10	CISCO	10/21/2010	/	Baik	Aset TI
917	3100202015	Auto Switch/Data Switch	11	CISCO	10/21/2010	/	Baik	Aset TI
918	3100202015	Auto Switch/Data Switch	12	CISCO	10/21/2010	/	Baik	Aset TI
919	3100202015	Auto Switch/Data Switch	13	CISCO	10/21/2010	/	Baik	Aset TI
920	3100202015	Auto Switch/Data Switch	14	CISCO	10/21/2010	/	Baik	Aset TI
921	3100202015	Auto Switch/Data Switch	15	CISCO	10/21/2010	/	Baik	Aset TI
922	3100202015	Auto Switch/Data Switch	16	CISCO	10/21/2010	/	Baik	Aset TI
923	3100202015	Auto Switch/Data Switch	17	CISCO	10/21/2010	/	Baik	Aset TI
924	3100202015	Auto Switch/Data Switch	18	CISCO	10/21/2010	/	Baik	Aset TI
925	3100202015	Auto Switch/Data Switch	19	CISCO	10/21/2010	/	Baik	Aset TI
926	3100202015	Auto Switch/Data Switch	20	CISCO	10/21/2010	/	Baik	Aset TI
927	3100202015	Auto Switch/Data Switch	21	CISCO	10/21/2010	/	Baik	Aset TI
928	3100202015	Auto Switch/Data Switch	22	CISCO	10/21/2010	/	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
929	3100202015	Auto Switch/Data Switch	23	CISCO	10/21/2010	/	Baik	Aset TI
930	3100202015	Auto Switch/Data Switch	24	CISCO	10/21/2010	/	Baik	Aset TI
931	3100202015	Auto Switch/Data Switch	25	CISCO	10/21/2010	/	Baik	Aset TI
932	3100202015	Auto Switch/Data Switch	26	CISCO	10/21/2010	/	Baik	Aset TI
933	3100202015	Auto Switch/Data Switch	27	CISCO	10/21/2010	/	Baik	Aset TI
934	3100202015	Auto Switch/Data Switch	28	CISCO	10/21/2010	/	Baik	Aset TI
935	3100202015	Auto Switch/Data Switch	29	CISCO	10/21/2010	/	Baik	Aset TI
936	3100202015	Auto Switch/Data Switch	30	CISCO	10/21/2010	/	Baik	Aset TI
937	3100202015	Auto Switch/Data Switch	31	CISCO	10/21/2010	/	Baik	Aset TI
938	3100202015	Auto Switch/Data Switch	32	CISCO	10/21/2010	/	Baik	Aset TI
939	3100202015	Auto Switch/Data Switch	33	CISCO	10/21/2010	/	Baik	Aset TI
940	3100202015	Auto Switch/Data Switch	34	CISCO	10/21/2010	/	Baik	Aset TI
941	3100202015	Auto Switch/Data Switch	35	CISCO	10/21/2010	/	Baik	Aset TI
942	3100202015	Auto Switch/Data Switch	36	CISCO	10/21/2010	/	Baik	Aset TI
943	3100202015	Auto Switch/Data Switch	37	CISCO	10/21/2010	/	Baik	Aset TI
944	3100202015	Auto Switch/Data Switch	38	CISCO	10/21/2010	/	Baik	Aset TI
945	3100202015	Auto Switch/Data Switch	39	CISCO	10/21/2010	/	Baik	Aset TI
946	3100202015	Auto Switch/Data Switch	40	CISCO	10/21/2010	/	Baik	Aset TI
947	3100202015	Auto Switch/Data Switch	41	CISCO	10/21/2010	/	Baik	Aset TI
948	3100202015	Auto Switch/Data Switch	42	CISCO	10/21/2010	/	Baik	Aset TI
949	3100202015	Auto Switch/Data Switch	43	CISCO	10/21/2010	/	Baik	Aset TI
950	3100202015	Auto Switch/Data Switch	44	CISCO	10/21/2010	/	Baik	Aset TI
951	3100202015	Auto Switch/Data Switch	45	CISCO	10/21/2010	/	Baik	Aset TI
952	3100202015	Auto Switch/Data Switch	46	CISCO	10/21/2010	/	Baik	Aset TI
953	3100202015	Auto Switch/Data Switch	47	CISCO	10/21/2010	/	Baik	Aset TI
954	3100202015	Auto Switch/Data Switch	48	CISCO	10/21/2010	/	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
955	3100202015	Auto Switch/Data Switch	49	CISCO	10/21/2010	/	Baik	Aset TI
956	3100202015	Auto Switch/Data Switch	50	CISCO	10/21/2010	/	Baik	Aset TI
957	3100202015	Auto Switch/Data Switch	51	CISCO	10/21/2010	/	Baik	Aset TI
958	3100202015	Auto Switch/Data Switch	52	CISCO	10/21/2010	/	Baik	Aset TI
959	3100202015	Auto Switch/Data Switch	53	CISCO	10/21/2010	/	Baik	Aset TI
960	3100202015	Auto Switch/Data Switch	54	CISCO	10/21/2010	/	Baik	Aset TI
961	3100202015	Auto Switch/Data Switch	55	HPE	12/26/2018	/	Baik	Aset TI
962	3100202015	Auto Switch/Data Switch	56	HPE	12/26/2018	/	Baik	Aset TI
963	3100202015	Auto Switch/Data Switch	57	HPE	12/26/2018	/	Baik	Aset TI
964	3100202015	Auto Switch/Data Switch	58	HPE	12/26/2018	/	Baik	Aset TI
965	3100202015	Auto Switch/Data Switch	59	HPE	12/26/2018	/	Baik	Aset TI
966	3100202015	Auto Switch/Data Switch	60	HPE	12/26/2018	/	Baik	Aset TI
967	3100202015	Auto Switch/Data Switch	61	HPE	12/26/2018	/	Baik	Aset TI
968	3100202015	Auto Switch/Data Switch	62	HPE	12/26/2018	/	Baik	Aset TI
969	3100202015	Auto Switch/Data Switch	63	HPE	12/26/2018	/	Baik	Aset TI
970	3100202015	Auto Switch/Data Switch	64	Cisco	12/28/2018	/	Baik	Aset TI
971	3100203001	CPU (Peralatan Personal Komputer)	1	APPLE New MAC Mini	12/21/2017	B02-2 /	Baik	Aset TI
972	3100203001	CPU (Peralatan Personal Komputer)	2	APPLE New MAC Mini	12/21/2017	B02-2 /	Baik	Aset TI
973	3100203001	CPU (Peralatan Personal Komputer)	3	Apple	12/31/2018	A05 /	Baik	Aset TI
974	3100203001	CPU (Peralatan Personal Komputer)	4	Apple	12/31/2018	B02-2 /	Baik	Aset TI
975	3100203001	CPU (Peralatan Personal Komputer)	5	Apple	12/31/2018	B02-2 /	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
976	3100203001	CPU (Peralatan Personal Komputer)	6	Apple	12/31/2018	B02-2 /	Baik	Aset TI
977	3100203001	CPU (Peralatan Personal Komputer)	7	Apple	12/31/2018	B02-2 /	Baik	Aset TI
978	3100203002	Monitor	1	LG	11/18/2015	A04-1 /	Baik	Aset TI
979	3100203002	Monitor	2	LG	11/18/2015	A04-1 /	Baik	Aset TI
980	3100203002	Monitor	3	LCD Monitor LG	8/31/2009	B02-2 /	Baik	Aset TI
981	3100203002	Monitor	4	Samsung 732 NW	4/30/2009	A05 /	Baik	Aset TI
982	3100203002	Monitor	5	LCD Samsung732 NW	6/23/2009	A05 /	Baik	Aset TI
983	3100203002	Monitor	6	Monitor LCD	3/24/2010	B02-2 /	Baik	Aset TI
984	3100203002	Monitor	7	Monitor LCD	3/24/2010	B02-2 /	Baik	Aset TI
985	3100203002	Monitor	8	LCD Monitotor	4/23/2010	B02-2 /	Baik	Aset TI
986	3100203002	Monitor	9	LCD Monitotor	4/23/2010	B02-2 /	Baik	Aset TI
987	3100203002	Monitor	10	LCD samsung	12/17/2009	B02-2 /	Baik	Aset TI
988	3100203002	Monitor	11	LG 22MP58	11/24/2017	B02-4 /	Baik	Aset TI
989	3100203002	Monitor	12	LG 22MP58	11/24/2017	B02-4 /	Baik	Aset TI
990	3100203003	Printer (Peralatan Personal Komputer)	1	HP/M176N	9/18/2015	B01 / R. IKTI	Baik	Aset TI
991	3100203003	Printer (Peralatan Personal Komputer)	8	EPSON LQ-2180	12/30/2003	B02-2 /	Rusak	Aset TI
992	3100203003	Printer (Peralatan Personal Komputer)	9	EPSON LQ-2180	12/30/2003	B02-2 /	Rusak	Aset TI
993	3100203003	Printer (Peralatan Personal Komputer)	10	HP LASERJET P2035N	4/21/2011	B02 /	Baik	Aset TI
994	3100203003	Printer (Peralatan Personal Komputer)	11	HP Color LaserJet CP2518n	6/27/2011	B02-2 /	Rusak	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
995	3100203003	Printer (Peralatan Personal Komputer)	12	Epson L100	3/8/2012	B02-2 /	Baik	Aset TI
996	3100203003	Printer (Peralatan Personal Komputer)	14	HP Laserjet 1102	12/5/2013	B02 /	Baik	Aset TI
997	3100203003	Printer (Peralatan Personal Komputer)	15	HP Officejet 150	12/11/2014	B02-2 /	Rusak	Aset TI
998	3100203003	Printer (Peralatan Personal Komputer)	16	Brother PT-E300VP	10/6/2016	B03 /	Baik	Aset TI
999	3100203003	Printer (Peralatan Personal Komputer)	17	HP/M-177FW	10/6/2016	B02-4 /	Baik	Aset TI
1000	3100203003	Printer (Peralatan Personal Komputer)	18	HP Laserjet M12w	12/31/2017	B02-2 /	Baik	Aset TI
1001	3100203003	Printer (Peralatan Personal Komputer)	19	Canon Pixma IP 110i	12/31/2017	B02-2 /	Rusak	Aset TI
1002	3100203003	Printer (Peralatan Personal Komputer)	20	Printer Epson L120	12/31/2017	B02-2 /	Baik	Aset TI
1003	3100203004	Scanner (Peralatan Personal Komputer)	1	Fujitsu SP25	7/10/2015	B02 /	Baik	Aset TI
1004	3100203004	Scanner (Peralatan Personal Komputer)	2	HP	12/11/2012	B02-2 /	Rusak	Aset TI
1005	3100203004	Scanner (Peralatan Personal Komputer)	3	Fujitsu	5/14/2014	B02 /	Baik	Aset TI
1006	3100203004	Scanner (Peralatan Personal Komputer)	4	Fujitsu	5/14/2014	B02-2 /	Rusak	Aset TI
1007	3100203004	Scanner (Peralatan Personal Komputer)	5	Fujitsu	5/14/2014	B02-2 /	Rusak	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
1008	3100203004	Scanner (Peralatan Personal Komputer)	6	Fujitsu	5/14/2014	B02-2 /	Rusak	Aset TI
1009	3100203004	Scanner (Peralatan Personal Komputer)	7	Fujitsu	5/14/2014	B02-2 /	Rusak	Aset TI
1010	3100203004	Scanner (Peralatan Personal Komputer)	8	Fujitsu ScanSnap S1300i	12/31/2017	B02-2 /	Baik	Aset TI
1011	3100203004	Scanner (Peralatan Personal Komputer)	9	Canon Scanner Lide 120	12/31/2017	/	Baik	Aset TI
1012	3100203017	External/ Portable Hardisk	1		8/31/2012	/	Rusak	Aset TI
1013	3100203017	External/ Portable Hardisk	2		8/31/2012	/	Rusak	Aset TI
1014	3100203017	External/ Portable Hardisk	3		8/31/2012	/	Rusak	Aset TI
1015	3100203017	External/ Portable Hardisk	4	WD MyCloud 8 TB	12/31/2017	B02-2 /	Baik	Aset TI
1016	3100204001	Server	1	HPE DL580 Gen9 CTO SVR	10/19/2017	B01-2 /	Baik	Aset TI
1017	3100204001	Server	2	HPE DL580 Gen9 CTO SVR	10/19/2017	B01-2 /	Baik	Aset TI
1018	3100204001	Server	3	HPE DL380 Gen9 CTO Derver	10/19/2017	B01-2 /	Baik	Aset TI
1019	3100204001	Server	4	HPE DL380 Gen9 CTO Derver	10/19/2017	B01-2 /	Baik	Aset TI
1020	3100204001	Server	5	HPE DL380 Gen9 CTO Derver	10/19/2017	B01-2 /	Baik	Aset TI
1021	3100204001	Server	6	HPE DL380 Gen9 CTO Derver	10/19/2017	B01-2 /	Baik	Aset TI
1022	3100204001	Server	7	HPE MSA 2040 SAN	10/19/2017	B01-2 /	Baik	Aset TI
1023	3100204001	Server	8	Server Merk Altos	11/11/2002	VI.4 / Gd Perpustakaan	Rusak	Aset TI
1024	3100204001	Server	9	HP / PROLIANT ML150	1/1/2005	/	Baik	Aset TI
1025	3100204001	Server	10	HP / PROLIANT ML150	1/1/2005	/	Baik	Aset TI
1026	3100204001	Server	11	Xeon	1/1/2005	B02-2 /	Baik	Aset TI
1027	3100204001	Server	12	HP / PROLIANT ML150	1/1/2005	/	Baik	Aset TI
1028	3100204001	Server	13	Advance Server SUN X4100	8/31/2009	B02-2 /	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
1029	3100204001	Server	14	Advance Server SUN X4100	8/31/2009	VI.3 / Data Center Gd Perpustakaan	Baik	Aset TI
1030	3100204001	Server	15	HP PROLIANT DL380G6	6/8/2010	B02-2 /	Baik	Aset TI
1031	3100204001	Server	16	CISCO	10/21/2010	B02-2 /	Baik	Aset TI
1032	3100204001	Server	17	Intel Xeon 6C ProcesorX5670	12/10/2010	B02-2 /	Baik	Aset TI
1033	3100204001	Server	18	HPPROLIANT DL 145 R G3,AMD OPTERON2.2 GHZ.MON 15	12/30/2010	B02-2 /	Baik	Aset TI
1034	3100204001	Server	19	HPPROLIANT DL 145 R G3,AMD OPTERON2.2 GHZ.MON 15	12/30/2010	B02-2 /	Baik	Aset TI
1035	3100204001	Server	20	HPPROLIANT DL 145 R G3,AMD OPTERON2.2 GHZ.MON 15	12/30/2010	B02-2 /	Baik	Aset TI
1036	3100204001	Server	21	HPPROLIANT DL 145 R G3,AMD OPTERON2.2 GHZ.MON 15	12/30/2010	B02-2 /	Baik	Aset TI
1037	3100204001	Server	22	Server Web & Download	6/27/2011	B01-2 /	Baik	Aset TI
1038	3100204001	Server	23	Server Web & Download	6/27/2011	B01-2 /	Baik	Aset TI
1039	3100204001	Server	24	Server Web & Download	6/27/2011	B01-2 /	Baik	Aset TI
1040	3100204001	Server	25	Server Web & Download	6/27/2011	B01-2 /	Baik	Aset TI
1041	3100204001	Server	26	Server Web & Download	6/27/2011	B01-2 /	Baik	Aset TI
1042	3100204001	Server	27	Server seleksi & Alokasi	6/27/2011	B01-2 /	Baik	Aset TI
1043	3100204001	Server	28	UPS ICA RN 3200C	6/27/2011	B03-2 /	Baik	Aset TI
1044	3100204001	Server	29	UPS ICA RN 3200C	6/27/2011	B03-2 /	Baik	Aset TI
1045	3100204001	Server	30	UPS ICA RN 3200C	6/27/2011	B03-2 /	Baik	Aset TI
1046	3100204001	Server	31	HP DL580R07 CTO Chassis (Database)	6/27/2011	B02-2 /	Baik	Aset TI
1047	3100204001	Server	32	HP DL380E	12/31/2012	B01-2 /	Baik	Aset TI
1048	3100204001	Server	33	HP DL380E	12/31/2012	B01-2 /	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
1049	3100204001	Server	34	HP DL380E	12/31/2012	B01-2 /	Baik	Aset TI
1050	3100204001	Server	35	HP	12/11/2012	B02-2 /	Baik	Aset TI
1051	3100204001	Server	36	HP/Proliant DL380G7	7/18/2012	/	Baik	Aset TI
1052	3100204001	Server	37	HP/Proliant DL380G7	7/18/2012	/	Baik	Aset TI
1053	3100204001	Server	38	HP/DL580	12/10/2014	B01-2 /	Baik	Aset TI
1054	3100204001	Server	39	HP/DL580	12/10/2014	B01-2 /	Baik	Aset TI
1055	3100204001	Server	40	DELL/PowerEdge R230	10/31/2016	B01-2 /	Baik	Aset TI
1056	3100204001	Server	41	HPE/Proliant DL580 Gen10	10/15/2018	/	Baik	Aset TI
1057	3100204001	Server	42	HPE/ProLiant DL380 Gen10	10/15/2018	/	Baik	Aset TI
1058	3100204001	Server	43	HPE/ProLiant DL380 Gen10	10/15/2018	/	Baik	Aset TI
1059	3100204001	Server	44	HPE/ProLiant DL380 Gen10	10/15/2018	/	Baik	Aset TI
1060	3100204001	Server	45	HPE/ProLiant DL380 Gen10	10/15/2018	/	Baik	Aset TI
1061	3100204001	Server	46	HPE/ProLiant DL360 Gen10	10/15/2018	B01-2 /	Baik	Aset TI
1062	3100204002	Router	1	Router	8/31/2009	B02-2 /	Baik	Aset TI
1063	3100204002	Router	2	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI
1064	3100204002	Router	3	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI
1065	3100204002	Router	4	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI
1066	3100204002	Router	5	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI
1067	3100204002	Router	6	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI
1068	3100204002	Router	7	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
1069	3100204002	Router	8	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI
1070	3100204002	Router	9	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI
1071	3100204002	Router	10	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI
1072	3100204002	Router	11	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI
1073	3100204002	Router	12	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI
1074	3100204002	Router	13	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI
1075	3100204002	Router	14	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI
1076	3100204002	Router	15	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI
1077	3100204002	Router	16	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI
1078	3100204002	Router	17	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI
1079	3100204002	Router	18	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI
1080	3100204002	Router	19	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI
1081	3100204002	Router	20	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
1082	3100204002	Router	21	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI
1083	3100204002	Router	22	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI
1084	3100204002	Router	23	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI
1085	3100204002	Router	24	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI
1086	3100204002	Router	25	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI
1087	3100204002	Router	26	WIFI LYNSYS,ADSL 2+ROUTER MODEM,ACCES POINT	12/30/2010	/	Rusak	Aset TI
1088	3100204002	Router	27	Gigabit Router Cisco 3945	6/27/2011	B02-2 /	Baik	Aset TI
1089	3100204002	Router	28	CISCO 7606 S	12/31/2012	B01-2 /	Baik	Aset TI
1090	3100204002	Router	29	Cisco ASR 1002X	10/3/2016	VI.3 / Data Center Gd Perpustakaan	Baik	Aset TI
1091	3100204002	Router	30	Mikrotik	12/21/2018	B01-2 /	Baik	Aset TI
1092	3100204014	Rak Server	1	Fortuna	3/10/2017	B02-2 /	Baik	Aset TI
1093	3100204014	Rak Server	2	Fortuna	3/10/2017	B02-2 /	Baik	Aset TI
1094	3100204014	Rak Server	3	Fortuna	3/10/2017	B02-2 /	Baik	Aset TI
1095	3100204014	Rak Server	4	Fortuna	3/10/2017	B02-2 /	Baik	Aset TI
1096	3100204014	Rak Server	5		11/4/2016	B02-2 /	Baik	Aset TI
1097	3100204015	Firewall	1	Barracuda 641 ADC	10/19/2017	B01-2 /	Baik	Aset TI
1098	3100204015	Firewall	2	Barracuda 641 ADC	10/19/2017	B01-2 /	Baik	Aset TI
1099	3100204015	Firewall	3	Barracuda 641 ADC	10/19/2017	B01-2 /	Baik	Aset TI
1100	3100204015	Firewall	4	Barracuda 641 ADC	10/19/2017	B01-2 /	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
1101	3100204015	Firewall	5	Firewall Cisco ASA 5585-X	6/27/2011	B01-2 /	Baik	Aset TI
1102	3100204023	Wireless Access Point	1	Cisco/AIR-CAP2702I-F	11/28/2016	/	Baik	Aset TI
1103	3100204023	Wireless Access Point	2	Cisco/AIR-CAP2702I-F	11/28/2016	B01-3 /	Baik	Aset TI
1104	3100204023	Wireless Access Point	3	Cisco/AIR-CAP2702I-F	11/28/2016	B01-3 /	Baik	Aset TI
1105	3100204023	Wireless Access Point	4	Cisco/AIR-CAP2702I-F	11/28/2016	B01-3 /	Baik	Aset TI
1106	3100204023	Wireless Access Point	5	Cisco/AIR-CAP2702I-F	11/28/2016	B01-3 /	Baik	Aset TI
1107	3100204023	Wireless Access Point	6	CISCO Aironet 1852E	12/21/2017	B01-3 /	Baik	Aset TI
1108	3100204023	Wireless Access Point	7	CISCO Aironet 1852E	12/21/2017	B01-3 /	Baik	Aset TI
1109	3100204023	Wireless Access Point	8	CISCO Aironet 1852E	12/21/2017	B01-3 /	Baik	Aset TI
1110	3100204023	Wireless Access Point	9	CISCO Aironet 3802E	12/21/2017	B01-3 /	Baik	Aset TI
1111	3100204023	Wireless Access Point	10	CISCO Aironet 3802E	12/21/2017	B01-3 /	Baik	Aset TI
1112	3100204023	Wireless Access Point	11	CISCO Aironet 3802E	12/21/2017	B01-3 /	Baik	Aset TI
1113	3100204024	Switch	1	HP	8/25/2017	B02-2 /	Baik	Aset TI
1114	3100204024	Switch	2	HP	8/25/2017	B02-2 /	Baik	Aset TI
1115	3100204024	Switch	3	Nexus N9K-C93120TX bundle 2pcs	10/19/2017	B01-2 / Data Center	Baik	Aset TI
1116	3100204024	Switch	4	Cisco Catalyst 3560X 24 Port	6/27/2011	B01-3 /	Baik	Aset TI
1117	3100204024	Switch	5	TP-Link	11/26/2013	B02-2 /	Baik	Aset TI
1118	3100204024	Switch	6	TP-Link	11/26/2013	B02-2 /	Baik	Aset TI
1119	3100204024	Switch	7	TP-Link	11/26/2013	B02-2 /	Baik	Aset TI
1120	3100204024	Switch	8	Cisco/WS-C4900M	12/10/2014	/	Baik	Aset TI
1121	3100204024	Switch	9	HP	12/5/2016	B02-2 /	Baik	Aset TI
1122	3100204024	Switch	10	HP	12/5/2016	B02-2 /	Baik	Aset TI
1123	3100204024	Switch	11	HPE/FlexFabric 5940	10/15/2018	/	Baik	Aset TI
1124	3100204027	Rackmount	1	INDORACK	12/3/2018	B02-2 /	Baik	Aset TI
1125	3100204027	Rackmount	2	INDORACK	12/3/2018	B02-2 /	Baik	Aset TI
1126	3100204027	Rackmount	3	INDORACK	12/3/2018	B02-2 /	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
1127	3100204027	Rackmount	4	INDORACK	12/3/2018	B02-2 /	Baik	Aset TI
1128	3100204028	KVM Keyboard Video Monitor	1	HPE KVM IP Cnsl G2 VM CAC SW	10/19/2017	B01-2 /	Baik	Aset TI
1129	3100204999	Peralatan Jaringan Lainnya	1	STORAGE AREA NETWORKS HP P2	12/31/2012	B01-2 /	Baik	Aset TI
1130	3100299999	Peralatan Komputer Lainnya	1	RB 1100 HX2	11/26/2013	B02-2 /	Baik	Aset TI
1131	3100299999	Peralatan Komputer Lainnya	2	RB 1100 HX2	11/26/2013	B01-2 /	Baik	Aset TI
1132	3100299999	Peralatan Komputer Lainnya	3	RB 1100 HX2	11/26/2013	B02-2 /	Baik	Aset TI
1133	3100299999	Peralatan Komputer Lainnya	4	SD Ram	12/5/2013	/	Rusak	Aset Non TI
1134	3100299999	Peralatan Komputer Lainnya	5	SD Ram	12/5/2013	/	Rusak	Aset Non TI
1135	3150405006	Air Conditioning (AC)	1	Panasonic	8/28/2012	B02-2 /	Baik	Aset TI
1136	3150405006	Air Conditioning (AC)	2	Panasonic	8/28/2012	B02-2 /	Baik	Aset TI
1137	3190102001	Alat Tenis Meja	1	Double Fish	1/28/2013	B03 / R Validasi	Baik	Aset Non TI
1138	3190103005	Peralatan Fitnes	1	Tredmill	1/1/2004	B03 / R Validasi	Baik	Aset Non TI
1139	3190103005	Peralatan Fitnes	2		1/1/2004	B03 / R Validasi	Baik	Aset Non TI
1140	8010101001	Software Komputer	1	Academic VMware vSphere 6	10/19/2017	B02-2 /	Baik	Aset TI
1141	8010101001	Software Komputer	2	Academic VMware vSphere 6	10/19/2017	B02-2 /	Baik	Aset TI
1142	8010101001	Software Komputer	3	Academic VMware vSphere 6	10/19/2017	B02-2 /	Baik	Aset TI
1143	8010101001	Software Komputer	4	Academic VMware vSphere 6	10/19/2017	B02-2 /	Baik	Aset TI
1144	8010101001	Software Komputer	5	Academic VMware vSphere 6	10/19/2017	B02-2 /	Baik	Aset TI
1145	8010101001	Software Komputer	6	Academic VMware vSphere 6	10/19/2017	B02-2 /	Baik	Aset TI
1146	8010101001	Software Komputer	7	Academic VMware vSphere 6	10/19/2017	B02-2 /	Baik	Aset TI
1147	8010101001	Software Komputer	8	Academic VMware vSphere 6	10/19/2017	B02-2 /	Baik	Aset TI
1148	8010101001	Software Komputer	9	SQLSvrStd ALNG LicSAPk	9/25/2015	B02-2 /	Baik	Aset TI
1149	8010101001	Software Komputer	10	WinSvrDataCtr ALNG LicSAPk	9/25/2015	B02-2 /	Baik	Aset TI
1150	8010101001	Software Komputer	11	WinSvrStd ALNG LicSAPk	9/25/2015	B02-2 /	Baik	Aset TI
1151	8010101001	Software Komputer	12	WinSvrCAL ALNG LicSAPK	9/25/2015	B02-2 /	Baik	Aset TI
1152	8010101001	Software Komputer	13	VSProwMSDN ALNG LicSAPk	9/25/2015	B02-2 /	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
1153	8010101001	Software Komputer	14	VisioPro ALNG LicSAPk	9/25/2015	B02-2 /	Baik	Aset TI
1154	8010101001	Software Komputer	15	SQLCAL ALNG LicSAPk	9/25/2015	B02-2 /	Baik	Aset TI
1155	8010101001	Software Komputer	16	WinEntforSA ALNG UpgrdSAPk	9/25/2015	B02-2 /	Baik	Aset TI
1156	8010101001	Software Komputer	17	OfficeProPlusEdu ALNG LicSAPk	9/25/2015	B02-2 /	Baik	Aset TI
1157	8010101001	Software Komputer	18	Software IT Governance	12/30/2010	B02-2 /	Baik	Aset TI
1158	8010101001	Software Komputer	19	SOFTWARE MAINTENANCE & SECURITY KEGIATAN IF-3	12/30/2010	B02-2 /	Baik	Aset TI
1159	8010101001	Software Komputer	20	SOFTWARE DECISION SUPPORT SYSTEM (DSS)	12/30/2010	B02-2 /	Baik	Aset TI
1160	8010101001	Software Komputer	21	Adobe Creative Suite 5 Master	6/27/2011	B02-2 /	Baik	Aset TI
1161	8010101001	Software Komputer	22	Adobe Creative Suite 5 Master	6/27/2011	B02-2 /	Baik	Aset TI
1162	8010101001	Software Komputer	23	Adobe Creative Suite 5 Master	6/27/2011	B02-2 /	Baik	Aset TI
1163	8010101001	Software Komputer	24	Adobe Creative Suite 5 Master	6/27/2011	B02-2 /	Baik	Aset TI
1164	8010101001	Software Komputer	25	Adobe Creative Suite 5 Master	6/27/2011	B02-2 /	Baik	Aset TI
1165	8010101001	Software Komputer	26	ApexSQL Universal Studio	6/27/2011	B02-2 /	Baik	Aset TI
1166	8010101001	Software Komputer	27	Microsoft SQL Server Enterprise	6/27/2011	B02-2 /	Baik	Aset TI
1167	8010101001	Software Komputer	28	Microsoft Windows Server	6/27/2011	B02-2 /	Baik	Aset TI
1168	8010101001	Software Komputer	29	Microsoft Windows Server	6/27/2011	B02-2 /	Baik	Aset TI
1169	8010101001	Software Komputer	30	ADOBE CREATIVE SUITE 5 MASTER COLLECTION	6/27/2011	B02-2 /	Baik	Aset TI
1170	8010101001	Software Komputer	31	ADOBE CREATIVE SUITE 5 MASTER COLLECTION	6/27/2011	B02-2 /	Baik	Aset TI
1171	8010101001	Software Komputer	32	ADOBE CREATIVE SUITE 5 MASTER COLLECTION	6/27/2011	B02-2 /	Baik	Aset TI
1172	8010101001	Software Komputer	33	ADOBE CREATIVE SUITE 5 MASTER COLLECTION	6/27/2011	B02-2 /	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
1173	8010101001	Software Komputer	34	ADOBE CREATIVE SUITE 5 MASTER COLLECTION	6/27/2011	B02-2 /	Baik	Aset TI
1174	8010101001	Software Komputer	35	ApexSQLUniversal Studio	6/27/2011	B02-2 /	Baik	Aset TI
1175	8010101001	Software Komputer	36	Microsoft SQL Server Enterprise 2008	6/27/2011	B02-2 /	Baik	Aset TI
1176	8010101001	Software Komputer	37	Microsoft Windowws Server Enterprise	6/27/2011	B02-2 /	Baik	Aset TI
1177	8010101001	Software Komputer	38	Microsoft Windowws Server Enterprise	6/27/2011	B02-2 /	Baik	Aset TI
1178	8010101001	Software Komputer	39	Software Pendukung Manaj.	9/17/2012	B02-2 /	Baik	Aset TI
1179	8010101001	Software Komputer	40	ADOBE	12/12/2012	B02-2 /	Baik	Aset TI
1180	8010101001	Software Komputer	41	ADOBE	12/12/2012	B02-2 /	Baik	Aset TI
1181	8010101001	Software Komputer	42	Adobe	12/12/2012	B02-2 /	Baik	Aset TI
1182	8010101001	Software Komputer	43	Streaming system	12/17/2012	B02-2 /	Baik	Aset TI
1183	8010101001	Software Komputer	44	VMWare/Sofware	7/18/2012	/	Baik	Aset TI
1184	8010101001	Software Komputer	45	Software Sistem Reservasi Online	12/6/2013	B02-2 /	Baik	Aset TI
1185	8010101001	Software Komputer	46	SIM Kinerja	5/30/2014	B02-2 /	Baik	Aset TI
1186	8010101001	Software Komputer	47	SIM kearsipan	8/14/2014	B02-2 /	Baik	Aset TI
1187	8010101001	Software Komputer	48	VM Ware	12/10/2014	B01-2 /	Baik	Aset TI
1188	8010101001	Software Komputer	49	Modul Tugas Belajar Dosen	11/28/2014	B02-2 /	Baik	Aset TI
1189	8010101001	Software Komputer	50	Apex SQL	11/27/2017	B02-2 /	Baik	Aset TI
1190	8010101001	Software Komputer	51	PDDIKTI Integrator	7/9/2018	A05 / R Layanan TSI	Baik	Aset TI
1191	8010101001	Software Komputer	52	PHP Maker v2018.0.8	8/15/2018	B02-2 /	Baik	Aset TI
1192	8010101001	Software Komputer	53	VMware	10/15/2018	B02-2 /	Baik	Aset TI
1193	8010101001	Software Komputer	54	VMware	10/15/2018	B02-2 /	Baik	Aset TI
1194	8010101001	Software Komputer	55	VMware	10/15/2018	B02-2 /	Baik	Aset TI
1195	8010101001	Software Komputer	56	VMware	10/15/2018	B02-2 /	Baik	Aset TI

No	Kode Barang	Barang	NUP	Merk/Type	Tgl. Perolehan	Lokasi	Kondisi	Aset TI / Non TI
1196	8010101001	Software Komputer	57	VMware	10/15/2018	B02-2 /	Baik	Aset TI
1197	8010101001	Software Komputer	58	VMware	10/15/2018	B02-2 /	Baik	Aset TI
1198	8010101001	Software Komputer	59	VMware	10/15/2018	B02-2 /	Baik	Aset TI
1199	8010101001	Software Komputer	60	VMware	10/15/2018	B02-2 /	Baik	Aset TI
1200	8010101001	Software Komputer	61	Fortinet	12/31/2018	B01 / R Staf IKTI	Baik	Aset TI
1201	8010101002	Lisensi	1	iThenticate	9/25/2015	B01 / R Staf IKTI	Baik	Aset TI
1202	8010101999	Aset Tak Berwujud Lainnya	1	Certificate SSL Verisign	6/27/2011		Baik	Aset TI
1203	8010101999	Aset Tak Berwujud Lainnya	2	Certificate SSL Verisign	6/27/2011	/	Baik	Aset TI
1204	3050201002	Meja Kerja Kayu	1		11/11/2002	A05-1 /	Baik	Aset Non TI
1205	3050201009	Meja Komputer	62			A05 /	Baik	Aset Non TI
1206	3050201009	Meja Komputer	63			A05 /	Baik	Aset Non TI
1207	3050201009	Meja Komputer	44			A05-2 /	Baik	Aset Non TI
1208	3060201001	Telephone (PABX)	1			A05-2 /	Baik	Aset Non TI
1209	3050105010	White Board	1			A05-3 /	Baik	Aset Non TI
1210	3050104005	Filing Cabinet Besi	1			B01 /	Baik	Aset Non TI
1211	3050204001	Lemari Es	2			B01-3 /	Baik	Aset Non TI
1212	3050201002	Meja Kerja Kayu	31			B03 /	Baik	Aset Non TI

* Warna merah menandakan aset dalam kondisi rusak

Lampiran C

Penghitungan Nilai Aset (*Asset Values*) pada aset TIK pada dikelola oleh DPTSI ITS

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
1	DPTSI	BAPKM	SI Akademik	1				Information System	3	4	3	10
2	DPTSI	BAPKM	SI Pendaftaran Seleksi Masuk ITS (SIMITS)	2				Information System	0	2	2	4
3	DPTSI	BAPKM	SI Pendataan Mahasiswa Baru ITS (SIPMABA)	3				Information System	1	2	2	5
4	DPTSI	DIRKEM	SIM Kemahasiswaan (SKEM)	4				Information System	1	1	2	4
5	DPTSI	DSDMO	SI Satuan Angka Kredit (SAR Online)	5				Information System	1	2	2	5
6	DPTSI	BAPKM	SI Yudisium	6				Information System	1	2	1	4
7	DPTSI	BAPKM	Modular SI Kurikulum	7				Information System	1	2	1	4
8	DPTSI	BAPKM	SI Penjadwalan Ruang (SIMARU)	8				Information System	1	2	1	4
9	DPTSI	DIRKEM	SI Beasiswa	9				Information System	1	2	1	4
10	DPTSI	DIRPAL	SI Perencanaan, Monitoring dan Evaluasi (SIPMONEV)	10				Information System	1	2	1	4
11	DPTSI	Biro Keuangan	SIM Rencana Belanja Anggaran (SIM RBA)	11				Information System	2	3	2	7
12	DPTSI	Biro Keuangan	SIM Keuangan	12				Information System	2	3	4	9
13	DPTSI	DIRPAL	SI Monitoring Pendapatan ITS (SIMONDITS)	13				Information System	2	3	4	9

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
14	DPTSI	DPPSP	SI Asrama	14				Information System	1	2	2	5
15	DPTSI	Biro Keuangan	Host-to-host App	15				Information System	2	3	4	9
16	DPTSI	Biro Umum	ePerkantoran	16				Information System	1	2	2	5
17	DPTSI	Biro Umum	SIM Kepegawaian	17				Information System	2	3	3	8
18	DPTSI	DSDMO	SIM Entry SK	18				Information System	1	2	2	5
19	DPTSI	DSDMO	SIM Penilaian Kinerja Tendik dan Dosen	19				Information System	1	3	2	6
20	DPTSI	DSDMO	SIM Insentif Kinerja (IKITS)	20				Information System	1	3	2	6
21	DPTSI	DIRPAL	Sistem ODOO ERP	21				Information System	1	2	1	4
22	DPTSI	Biro Keuangan	SIM Persediaan	22				Information System	1	3	1	5
23	DPTSI	Biro Keuangan	SIM Inventori (E-Aset)	23				Information System	1	3	1	5
24	DPTSI	DPTSI	Ad Hoc Reporting	24				Information System	1	1	1	3
25	DPTSI	DPTSI	Sistem Informasi Pelaporan Data	25				Information System	2	2	3	7
26	DPTSI	DPTSI	Executive Reporting	26				Information System	2	2	3	7
27	DPTSI	LPPM	SIM Penelitian ITS (SIMPel)	27				Information System	1	2	1	4
28	DPTSI	LPPM	SI Resource ITS (RESITS)	28				Information System	0	1	1	2

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
29	DPTSI	P2K2M	ITS Alumni Data Tracking System	29				Information System	1	1	1	3
30	DPTSI	DPTSI	Service Desk ITS (E-ticket)	30				Information System	1	1	1	3
31	DPTSI	DSDMO	SIM Kepangkatan (SIKEPANG)	31				Information System	1	2	1	4
32	DPTSI	DIRAKAD	SIM Beban Kerja Dosen (BKD)	32				Information System	1	2	1	4
33	DPTSI	DPTSI	Single Sign On (SSO) App	33				Information System	4	4	4	12
34	DPTSI	Biro Umum	SIM Kearsipan	34				Information System	1	2	1	4
35	DPTSI	DIRAKAD	PDDIKTI Integrator	35				Information System	1	2	1	4
36	DPTSI	SekITS	ITS Website	36				Information System	0	1	4	5
37	DPTSI	BAPKM	SI Presensi Online	37				Information System	1	2	3	6
38	DPTSI	DPTSI	Software DAAS MOD	1	Software Pengemb. Sistem Infor Manj (CMMS)	2010		Software	1	2	2	5
39	DPTSI	DPTSI	Software Komputer	1	Academic VMware vSphere 6	2017		Software	1	2	2	5
40	DPTSI	DPTSI	Software Komputer	2	Academic VMware vSphere 6	2017		Software	1	2	2	5
41	DPTSI	DPTSI	Software Komputer	3	Academic VMware vSphere 6	2017		Software	1	2	2	5
42	DPTSI	DPTSI	Software Komputer	4	Academic VMware vSphere 6	2017		Software	1	2	2	5
43	DPTSI	DPTSI	Software Komputer	5	Academic VMware vSphere 6	2017		Software	1	2	2	5

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
44	DPTSI	DPTSI	Software Komputer	6	Academic VMware vSphere 6	2017		Software	1	2	2	5
45	DPTSI	DPTSI	Software Komputer	7	Academic VMware vSphere 6	2017		Software	1	2	2	5
46	DPTSI	DPTSI	Software Komputer	8	Academic VMware vSphere 6	2017		Software	1	2	2	5
47	DPTSI	DPTSI	Software Komputer	9	SQLSvrStd ALNG LicSAPk	2015		Software	1	2	2	5
48	DPTSI	DPTSI	Software Komputer	10	WinSvrDataCtr ALNG LicSAPk	2015		Software	1	2	2	5
49	DPTSI	DPTSI	Software Komputer	11	WinSvrStd ALNG LicSAPk	2015		Software	1	2	2	5
50	DPTSI	DPTSI	Software Komputer	12	WinSvrCAL ALNG LicSAPK	2015		Software	1	2	2	5
51	DPTSI	DPTSI	Software Komputer	13	VSProwMSDN ALNG LicSAPk	2015		Software	1	2	2	5
52	DPTSI	DPTSI	Software Komputer	14	VisioPro ALNG LicSAPk	2015		Software	1	2	2	5
53	DPTSI	DPTSI	Software Komputer	15	SQLCAL ALNG LicSAPk	2015		Software	1	2	2	5
54	DPTSI	DPTSI	Software Komputer	16	WinEntforSA ALNG UpgrdSAPk	2015		Software	1	2	2	5
55	DPTSI	DPTSI	Software Komputer	17	OfficeProPlusEdu ALNG LicSAPk	2015		Software	1	2	2	5
56	DPTSI	DPTSI	Software Komputer	18	Software IT Governance	2010		Software	1	2	2	5
57	DPTSI	DPTSI	Software Komputer	19	SOFTWARE MAINTENANCE & SECURITY KEGIATAN IF-3	2010		Software	1	2	2	5

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
58	DPTSI	DPTSI	Software Komputer	20	SOFTWARE DECISION SUPPORT SYSTEM (DSS)	2010		Software	1	2	2	5
59	DPTSI	DPTSI	Software Komputer	21	Adobe Creative Suite 5 Master	2011		Software	1	2	2	5
60	DPTSI	DPTSI	Software Komputer	22	Adobe Creative Suite 5 Master	2011		Software	1	2	2	5
61	DPTSI	DPTSI	Software Komputer	23	Adobe Creative Suite 5 Master	2011		Software	1	2	2	5
62	DPTSI	DPTSI	Software Komputer	24	Adobe Creative Suite 5 Master	2011		Software	1	2	2	5
63	DPTSI	DPTSI	Software Komputer	25	Adobe Creative Suite 5 Master	2011		Software	1	2	2	5
64	DPTSI	DPTSI	Software Komputer	26	ApexSQL Universal Studio	2011		Software	1	2	2	5
65	DPTSI	DPTSI	Software Komputer	27	Microsoft SQL Server Enterprise	2011		Software	1	2	2	5
66	DPTSI	DPTSI	Software Komputer	28	Microsoft Windows Server	2011		Software	1	2	2	5
67	DPTSI	DPTSI	Software Komputer	29	Microsoft Windows Server	2011		Software	1	2	2	5
68	DPTSI	DPTSI	Software Komputer	30	ADOBE CREATIVE SUITE 5 MASTER COLLECTION	2011		Software	1	2	2	5
69	DPTSI	DPTSI	Software Komputer	31	ADOBE CREATIVE SUITE 5 MASTER COLLECTION	2011		Software	1	2	2	5
70	DPTSI	DPTSI	Software Komputer	32	ADOBE CREATIVE SUITE 5 MASTER COLLECTION	2011		Software	1	2	2	5
71	DPTSI	DPTSI	Software Komputer	33	ADOBE CREATIVE SUITE 5 MASTER COLLECTION	2011		Software	1	2	2	5
72	DPTSI	DPTSI	Software Komputer	34	ADOBE CREATIVE SUITE 5 MASTER COLLECTION	2011		Software	1	2	2	5

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
73	DPTSI	DPTSI	Software Komputer	35	ApexSQLUniversal Studio	2011		Software	1	2	2	5
74	DPTSI	DPTSI	Software Komputer	36	Microsoft SQL Server Enterprise 2008	2011		Software	1	2	2	5
75	DPTSI	DPTSI	Software Komputer	37	Microsoft Windowws Server Enterprise	2011		Software	1	2	2	5
76	DPTSI	DPTSI	Software Komputer	38	Microsoft Windowws Server Enterprise	2011		Software	1	2	2	5
77	DPTSI	DPTSI	Software Komputer	39	Software Pendukung Manaj.	2012		Software	1	2	2	5
78	DPTSI	DPTSI	Software Komputer	40	ADOBE	2012		Software	1	2	2	5
79	DPTSI	DPTSI	Software Komputer	41	ADOBE	2012		Software	1	2	2	5
80	DPTSI	DPTSI	Software Komputer	42	Adobe	2012		Software	1	2	2	5
81	DPTSI	DPTSI	Software Komputer	43	Streaming system	2012		Software	1	2	2	5
82	DPTSI	DPTSI	Software Komputer	44	VMWare/Sofware	2012		Software	1	2	2	5
83	DPTSI	DPTSI	Software Komputer	45	Software Sistem Reservasi Online	2013		Software	1	2	2	5
84	DPTSI	DPTSI	Software Komputer	46	SIM Kinerja	2014		Software	1	2	2	5
85	DPTSI	DPTSI	Software Komputer	47	SIM kearsipan	2014		Software	1	2	2	5
86	DPTSI	DPTSI	Software Komputer	48	VM Ware	2014		Software	1	2	2	5
87	DPTSI	DPTSI	Software Komputer	49	Modul Tugas Belajar Dosen	2014		Software	1	2	2	5

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
88	DPTSI	DPTSI	Software Komputer	50	Apex SQL	2017		Software	1	2	2	5
89	DPTSI	DPTSI	Software Komputer	51	PDDIKTI Integrator	2018		Software	1	2	2	5
90	DPTSI	DPTSI	Software Komputer	52	PHP Maker v2018.0.8	2018		Software	1	2	2	5
91	DPTSI	DPTSI	Software Komputer	53	VMware	2018		Software	1	2	2	5
92	DPTSI	DPTSI	Software Komputer	54	VMware	2018		Software	1	2	2	5
93	DPTSI	DPTSI	Software Komputer	55	VMware	2018		Software	1	2	2	5
94	DPTSI	DPTSI	Software Komputer	56	VMware	2018		Software	1	2	2	5
95	DPTSI	DPTSI	Software Komputer	57	VMware	2018		Software	1	2	2	5
96	DPTSI	DPTSI	Software Komputer	58	VMware	2018		Software	1	2	2	5
97	DPTSI	DPTSI	Software Komputer	59	VMware	2018		Software	1	2	2	5
98	DPTSI	DPTSI	Software Komputer	60	VMware	2018		Software	1	2	2	5
99	DPTSI	DPTSI	Software Komputer	61	Fortinet	2018		Software	1	2	2	5
100	DPTSI	DPTSI	Lisensi	1	iThenticate	2015		Software	1	2	2	5
101	DPTSI	DPTSI	Aset Tak Berwujud Lainnya	1	Certificate SSL Verisign	2011		Software	1	2	2	5
102	DPTSI	DPTSI	Aset Tak Berwujud Lainnya	2	Certificate SSL Verisign	2011		Software	1	2	2	5

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
103	DPTSI	DPTSI	Modulas Monitoring System	1	Modul	2009		Network Device	2	2	3	7
104	DPTSI	DPTSI	Fiber Optic Operating	1	GE	2010		Network Device	3	4	4	11
105	DPTSI	DPTSI	Panel Uto Power	1	Panel Listrik	2009		Network Device	1	2	3	6
106	DPTSI	DPTSI	Interface Network	1	CISCO	2010		Network Device	3	3	4	10
107	DPTSI	DPTSI	Paralel Control Network	1	CISCO	2010		Network Device	3	3	4	10
108	DPTSI	DPTSI	Internet Network	1	CISCO	2010		Network Device	3	3	4	10
109	DPTSI	DPTSI	Komputer Jaringan Lainnya	1	HP	2012		Network Device	3	3	4	10
110	DPTSI	DPTSI	KVM Keyboard Video Monitor	1	HPE KVM IP Cnsl G2 VM CAC SW	2017		Network Device	2	1	2	5
111	DPTSI	DPTSI	Server	1	HPE DL580 Gen9 CTO SVR	2017	OLTP server	Network Device	3	4	4	11
112	DPTSI	DPTSI	Server	2	HPE DL580 Gen9 CTO SVR	2017	OLAP Server	Network Device	3	4	4	11
113	DPTSI	DPTSI	Server	3	HPE DL380 Gen9 CTO Derver	2017	VMWare 65 Server	Network Device	3	4	4	11
114	DPTSI	DPTSI	Server	4	HPE DL380 Gen9 CTO Derver	2017	VMWare 65 Server	Network Device	3	4	4	11
115	DPTSI	DPTSI	Server	5	HPE DL380 Gen9 CTO Derver	2017	VMWare 65 Server	Network Device	3	4	4	11
116	DPTSI	DPTSI	Server	6	HPE DL380 Gen9 CTO Derver	2017	VMWare 65 Server	Network Device	3	4	4	11
117	DPTSI	DPTSI	Server	7	HPE MSA 2040 SAN	2017	VMWare 65 Server	Network Device	3	4	4	11

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
118	DPTSI	DPTSI	Server	9	HP / PROLIANT ML150	2005		Network Device	3	4	4	11
119	DPTSI	DPTSI	Server	10	HP / PROLIANT ML150	2005		Network Device	3	4	4	11
120	DPTSI	DPTSI	Server	11	Xeon	2005		Network Device	3	4	4	11
121	DPTSI	DPTSI	Server	12	HP / PROLIANT ML150	2005		Network Device	3	4	4	11
122	DPTSI	DPTSI	Server	13	Advance Server SUN X4100	2009		Network Device	3	4	4	11
123	DPTSI	DPTSI	Server	14	Advance Server SUN X4100	2009	Data Center	Network Device	3	4	4	11
124	DPTSI	DPTSI	Server	15	HP PROLIANT DL380G6	2010		Network Device	3	4	4	11
125	DPTSI	DPTSI	Server	16	CISCO	2010		Network Device	3	4	4	11
126	DPTSI	DPTSI	Server	17	Intel Xeon 6C ProcesorX5670	2010		Network Device	3	4	4	11
127	DPTSI	DPTSI	Server	18	HPPROLIANT DL 145 R G3,AMD OPTERON2.2 GHZ.MON 15	2010		Network Device	3	4	4	11
128	DPTSI	DPTSI	Server	19	HPPROLIANT DL 145 R G3,AMD OPTERON2.2 GHZ.MON 15	2010		Network Device	3	4	4	11
129	DPTSI	DPTSI	Server	20	HPPROLIANT DL 145 R G3,AMD OPTERON2.2 GHZ.MON 15	2010		Network Device	3	4	4	11
130	DPTSI	DPTSI	Server	21	HPPROLIANT DL 145 R G3,AMD OPTERON2.2 GHZ.MON 15	2010		Network Device	3	4	4	11
131	DPTSI	DPTSI	Server	22	Server Web & Download	2011		Network Device	3	4	4	11

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
132	DPTSI	DPTSI	Server	23	Server Web & Download	2011		Network Device	3	4	4	11
133	DPTSI	DPTSI	Server	24	Server Web & Download	2011		Network Device	3	4	4	11
134	DPTSI	DPTSI	Server	25	Server Web & Download	2011		Network Device	3	4	4	11
135	DPTSI	DPTSI	Server	26	Server Web & Download	2011		Network Device	3	4	4	11
136	DPTSI	DPTSI	Server	27	Server seleksi & Alokasi	2011		Network Device	3	4	4	11
137	DPTSI	DPTSI	Server	28	UPS ICA RN 3200C	2011	UPS Server	Network Device	3	4	4	11
138	DPTSI	DPTSI	Server	29	UPS ICA RN 3200C	2011	UPS Server	Network Device	3	4	4	11
139	DPTSI	DPTSI	Server	30	UPS ICA RN 3200C	2011	UPS Server	Network Device	3	4	4	11
140	DPTSI	DPTSI	Server	31	HP DL580R07 CTO Chassis (Database)	2011	Database Server	Network Device	3	4	4	11
141	DPTSI	DPTSI	Server	32	HP DL380E	2012	HyperV Server	Network Device	3	4	4	11
142	DPTSI	DPTSI	Server	33	HP DL380E	2012	HyperV Server	Network Device	3	4	4	11
143	DPTSI	DPTSI	Server	34	HP DL380E	2012	HyperV Server	Network Device	3	4	4	11
144	DPTSI	DPTSI	Server	35	HP	2012		Network Device	3	4	4	11
145	DPTSI	DPTSI	Server	36	HP/Proliant DL380G7	2012	Proxmox VE Server	Network Device	3	4	4	11
146	DPTSI	DPTSI	Server	37	HP/Proliant DL380G7	2012	Proxmox VE Server	Network Device	3	4	4	11

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
147	DPTSI	DPTSI	Server	38	HP/DL580	2014	VMWare 22 Server	Network Device	3	4	4	11
148	DPTSI	DPTSI	Server	39	HP/DL580	2014	VMWare 22 Server	Network Device	3	4	4	11
149	DPTSI	DPTSI	Server	40	DELL/PowerEdge R230	2016	Hosting zeus Server	Network Device	3	4	4	11
150	DPTSI	DPTSI	Server	41	HPE/Proliant DL580 Gen10	2018	Proxmox VE Server	Network Device	3	4	4	11
151	DPTSI	DPTSI	Server	42	HPE/ProLiant DL380 Gen10	2018	Proxmox VE Server	Network Device	3	4	4	11
152	DPTSI	DPTSI	Server	43	HPE/ProLiant DL380 Gen10	2018	Proxmox VE Server	Network Device	3	4	4	11
153	DPTSI	DPTSI	Server	44	HPE/ProLiant DL380 Gen10	2018	Proxmox VE Server	Network Device	3	4	4	11
154	DPTSI	DPTSI	Server	45	HPE/ProLiant DL380 Gen10	2018	Proxmox VE Server	Network Device	3	4	4	11
155	DPTSI	DPTSI	Server	46	HPE/ProLiant DL360 Gen10	2018	Proxmox VE Server	Network Device	3	4	4	11
156	DPTSI	DPTSI	Wireless Access Point	1	Cisco/AIR-CAP2702I-F	2016		Network Device	1	3	4	8
157	DPTSI	DPTSI	Wireless Access Point	2	Cisco/AIR-CAP2702I-F	2016		Network Device	1	3	4	8
158	DPTSI	DPTSI	Wireless Access Point	3	Cisco/AIR-CAP2702I-F	2016		Network Device	1	3	4	8
159	DPTSI	DPTSI	Wireless Access Point	4	Cisco/AIR-CAP2702I-F	2016		Network Device	1	3	4	8
160	DPTSI	DPTSI	Wireless Access Point	5	Cisco/AIR-CAP2702I-F	2016		Network Device	1	3	4	8
161	DPTSI	DPTSI	Wireless Access Point	6	CISCO Aironet 1852E	2017		Network Device	1	3	4	8

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
162	DPTSI	DPTSI	Wireless Access Point	7	CISCO Aironet 1852E	2017		Network Device	1	3	4	8
163	DPTSI	DPTSI	Wireless Access Point	8	CISCO Aironet 1852E	2017		Network Device	1	3	4	8
164	DPTSI	DPTSI	Wireless Access Point	9	CISCO Aironet 3802E	2017		Network Device	1	3	4	8
165	DPTSI	DPTSI	Wireless Access Point	10	CISCO Aironet 3802E	2017		Network Device	1	3	4	8
166	DPTSI	DPTSI	Wireless Access Point	11	CISCO Aironet 3802E	2017		Network Device	1	3	4	8
167	DPTSI	DPTSI	Firewall	1	Barracuda 641 ADC	2017	Network Firewall	Network Device	2	4	4	10
168	DPTSI	DPTSI	Firewall	2	Barracuda 641 ADC	2017	Network Firewall	Network Device	2	4	4	10
169	DPTSI	DPTSI	Firewall	3	Barracuda 641 ADC	2017	Network Firewall	Network Device	2	4	4	10
170	DPTSI	DPTSI	Firewall	4	Barracuda 641 ADC	2017	Network Firewall	Network Device	2	4	4	10
171	DPTSI	DPTSI	Firewall	5	Firewall Cisco ASA 5585-X	2011	Network Firewall	Network Device	2	4	4	10
172	DPTSI	DPTSI	Router	27	Gigabit Router Cisco 3945	2011		Network Device	2	4	3	9
173	DPTSI	DPTSI	Router	28	CISCO 7606 S	2012		Network Device	2	4	3	9
174	DPTSI	DPTSI	Router	29	Cisco ASR 1002X	2016	Core BGP router	Network Device	2	4	4	10
175	DPTSI	DPTSI	Router	30	Mikrotik	2018	Internet Access	Network Device	2	4	4	10
176	DPTSI	DPTSI	Router	1	RB 1100 HX2	2013	Internet Access	Network Device	2	4	4	10

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
177	DPTSI	DPTSI	Router	2	RB 1100 HX2	2013	Internet Access	Network Device	2	4	4	10
178	DPTSI	DPTSI	Router	3	RB 1100 HX2	2013	Internet Access	Network Device	2	4	4	10
179	DPTSI	DPTSI	Switcher/Patch Panel	1	Switch	2009	Distributor Switch	Network Device	2	4	4	10
180	DPTSI	DPTSI	Auto Switch/Data Switch	1	CISCO 4900	2010	Access Switch	Network Device	2	4	3	9
181	DPTSI	DPTSI	Auto Switch/Data Switch	2	CISCO 4900	2010	Access Switch	Network Device	2	4	3	9
182	DPTSI	DPTSI	Auto Switch/Data Switch	3	CISCO 4900	2010	Access Switch	Network Device	2	4	3	9
183	DPTSI	DPTSI	Auto Switch/Data Switch	4	CISCO 4900	2010	Access Switch	Network Device	2	4	3	9
184	DPTSI	DPTSI	Auto Switch/Data Switch	5	CISCO 4900	2010	Access Switch	Network Device	2	4	3	9
185	DPTSI	DPTSI	Auto Switch/Data Switch	6	CISCO 4900	2010	Access Switch	Network Device	2	4	3	9
186	DPTSI	DPTSI	Auto Switch/Data Switch	7	CISCO 4900	2010	Access Switch	Network Device	2	4	3	9
187	DPTSI	DPTSI	Auto Switch/Data Switch	8	CISCO 4900	2010	Access Switch	Network Device	2	4	3	9
188	DPTSI	DPTSI	Auto Switch/Data Switch	9	CISCO 4900	2010	Access Switch	Network Device	2	4	3	9
189	DPTSI	DPTSI	Auto Switch/Data Switch	10	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
190	DPTSI	DPTSI	Auto Switch/Data Switch	11	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
191	DPTSI	DPTSI	Auto Switch/Data Switch	12	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
192	DPTSI	DPTSI	Auto Switch/Data Switch	13	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
193	DPTSI	DPTSI	Auto Switch/Data Switch	14	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
194	DPTSI	DPTSI	Auto Switch/Data Switch	15	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
195	DPTSI	DPTSI	Auto Switch/Data Switch	16	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
196	DPTSI	DPTSI	Auto Switch/Data Switch	17	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
197	DPTSI	DPTSI	Auto Switch/Data Switch	18	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
198	DPTSI	DPTSI	Auto Switch/Data Switch	19	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
199	DPTSI	DPTSI	Auto Switch/Data Switch	20	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
200	DPTSI	DPTSI	Auto Switch/Data Switch	21	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
201	DPTSI	DPTSI	Auto Switch/Data Switch	22	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
202	DPTSI	DPTSI	Auto Switch/Data Switch	23	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
203	DPTSI	DPTSI	Auto Switch/Data Switch	24	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
204	DPTSI	DPTSI	Auto Switch/Data Switch	25	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
205	DPTSI	DPTSI	Auto Switch/Data Switch	26	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
206	DPTSI	DPTSI	Auto Switch/Data Switch	27	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
207	DPTSI	DPTSI	Auto Switch/Data Switch	28	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
208	DPTSI	DPTSI	Auto Switch/Data Switch	29	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
209	DPTSI	DPTSI	Auto Switch/Data Switch	30	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
210	DPTSI	DPTSI	Auto Switch/Data Switch	31	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
211	DPTSI	DPTSI	Auto Switch/Data Switch	32	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
212	DPTSI	DPTSI	Auto Switch/Data Switch	33	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
213	DPTSI	DPTSI	Auto Switch/Data Switch	34	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
214	DPTSI	DPTSI	Auto Switch/Data Switch	35	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
215	DPTSI	DPTSI	Auto Switch/Data Switch	36	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
216	DPTSI	DPTSI	Auto Switch/Data Switch	37	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
217	DPTSI	DPTSI	Auto Switch/Data Switch	38	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
218	DPTSI	DPTSI	Auto Switch/Data Switch	39	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
219	DPTSI	DPTSI	Auto Switch/Data Switch	40	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
220	DPTSI	DPTSI	Auto Switch/Data Switch	41	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
221	DPTSI	DPTSI	Auto Switch/Data Switch	42	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
222	DPTSI	DPTSI	Auto Switch/Data Switch	43	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
223	DPTSI	DPTSI	Auto Switch/Data Switch	44	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
224	DPTSI	DPTSI	Auto Switch/Data Switch	45	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
225	DPTSI	DPTSI	Auto Switch/Data Switch	46	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
226	DPTSI	DPTSI	Auto Switch/Data Switch	47	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
227	DPTSI	DPTSI	Auto Switch/Data Switch	48	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
228	DPTSI	DPTSI	Auto Switch/Data Switch	49	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
229	DPTSI	DPTSI	Auto Switch/Data Switch	50	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
230	DPTSI	DPTSI	Auto Switch/Data Switch	51	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
231	DPTSI	DPTSI	Auto Switch/Data Switch	52	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
232	DPTSI	DPTSI	Auto Switch/Data Switch	53	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
233	DPTSI	DPTSI	Auto Switch/Data Switch	54	CISCO 3560	2010	Access Switch	Network Device	2	4	3	9
234	DPTSI	DPTSI	Auto Switch/Data Switch	55	HPE 1820	2018	Access Switch	Network Device	2	4	3	9
235	DPTSI	DPTSI	Auto Switch/Data Switch	56	HPE 1820	2018	Access Switch	Network Device	2	4	3	9
236	DPTSI	DPTSI	Auto Switch/Data Switch	57	HPE 1820	2018	Access Switch	Network Device	2	4	3	9

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
237	DPTSI	DPTSI	Auto Switch/Data Switch	58	HPE 1820	2018	Access Switch	Network Device	2	4	3	9
238	DPTSI	DPTSI	Auto Switch/Data Switch	59	HPE 1820	2018	Access Switch	Network Device	2	4	3	9
239	DPTSI	DPTSI	Auto Switch/Data Switch	60	HPE 1820	2018	Access Switch	Network Device	2	4	3	9
240	DPTSI	DPTSI	Auto Switch/Data Switch	61	HPE 1820	2018	Access Switch	Network Device	2	4	3	9
241	DPTSI	DPTSI	Auto Switch/Data Switch	62	HPE 1820	2018	Access Switch	Network Device	2	4	3	9
242	DPTSI	DPTSI	Auto Switch/Data Switch	63	HPE 1820	2018	Access Switch	Network Device	2	4	3	9
243	DPTSI	DPTSI	Auto Switch/Data Switch	64	CISCO 3560	2018	Access Switch	Network Device	2	4	3	9
244	DPTSI	DPTSI	Switch	1	HP 1820	2017	Access Switch	Network Device	2	4	3	9
245	DPTSI	DPTSI	Switch	2	HP 1820	2017	Access Switch	Network Device	2	4	3	9
246	DPTSI	DPTSI	Switch	3	Nexus N9K-C93120TX bundle 2pcs	2017	Database Data Switch	Network Device	2	4	4	10
247	DPTSI	DPTSI	Switch	4	Cisco Catalyst 3560X 24 Port	2011	Access Switch	Network Device	2	4	3	9
248	DPTSI	DPTSI	Switch	5	TP-Link	2013	Access Switch	Network Device	2	4	3	9
249	DPTSI	DPTSI	Switch	6	TP-Link	2013	Access Switch	Network Device	2	4	3	9
250	DPTSI	DPTSI	Switch	7	TP-Link	2013	Access Switch	Network Device	2	4	3	9
251	DPTSI	DPTSI	Switch	8	Cisco/WS-C4900M	2014	Distributor Switch	Network Device	2	4	4	10

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
252	DPTSI	DPTSI	Switch	9	HP 1820	2016	Access Switch	Network Device	2	4	3	9
253	DPTSI	DPTSI	Switch	10	HP 1820	2016	Access Switch	Network Device	2	4	3	9
254	DPTSI	DPTSI	Switch	11	HPE/FlexFabric 5940	2018	Datacentre Access Switch	Network Device	2	4	4	10
255	DPTSI	DPTSI	Switch	12	Huawei 12700	2016	Core Switch	Network Device	2	4	4	10
256	DPTSI	DPTSI	Switch	13	Cisco 6500	2016	Core Switch	Network Device	2	4	4	10
257	DPTSI	DPTSI	Switch	14	Cisco 7700	2016	Core Switch	Network Device	2	4	4	10
258	DPTSI	DPTSI	Rak Server	1	Fortuna	2017		Network Device	1	2	2	5
259	DPTSI	DPTSI	Rak Server	2	Fortuna	2017		Network Device	1	2	2	5
260	DPTSI	DPTSI	Rak Server	3	Fortuna	2017		Network Device	1	2	2	5
261	DPTSI	DPTSI	Rak Server	4	Fortuna	2017		Network Device	1	2	2	5
262	DPTSI	DPTSI	Rak Server	5		2016		Network Device	1	2	2	5
263	DPTSI	DPTSI	Rackmount	1	INDORACK	2018		Network Device	1	2	2	5
264	DPTSI	DPTSI	Rackmount	2	INDORACK	2018		Network Device	1	2	2	5
265	DPTSI	DPTSI	Rackmount	3	INDORACK	2018		Network Device	1	2	2	5
266	DPTSI	DPTSI	Rackmount	4	INDORACK	2018		Network Device	1	2	2	5

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
267	DPTSI	DPTSI	Storage Modul Disk (Peralatan Mainframe)	1	SAN/Storage	2012		Storage Device	3	4	4	11
268	DPTSI	DPTSI	Storage Modul Disk (Peralatan Mainframe)	2	Hitachi/HUS110	2014		Storage Device	3	4	4	11
269	DPTSI	DPTSI	External/ Portable Hardisk	4	WD MyCloud 8 TB	2017		Storage Device	2	2	1	5
270	DPTSI	DPTSI	Peralatan Jaringan Lainnya	1	STORAGE AREA NETWORKS HP P2	2012		Storage Device	3	4	4	11
271	DPTSI	DPTSI	Telephone Mobile	1	Samsung	2017	App Testing Device	Hardware	1	2	1	4
272	DPTSI	DPTSI	Telephone Mobile	2	Samsung S8+	2017	App Testing Device	Hardware	1	2	1	4
273	DPTSI	DPTSI	Telephone Mobile	3	Apple iPhone 7 Plus	2017	App Testing Device	Hardware	1	2	1	4
274	DPTSI	DPTSI	Telephone Mobile	4	Apple iPhone 7 JetBlack	2017	App Testing Device	Hardware	1	2	1	4
275	DPTSI	DPTSI	Ultra Mobile P.C.	1	Apple iPad Wi-Fi	2017	App Testing Device	Hardware	1	2	1	4
276	DPTSI	DPTSI	Ultra Mobile P.C.	2	Samsung Tab3	2017	App Testing Device	Hardware	1	2	1	4
277	DPTSI	DPTSI	Lap Top	5	Mac Book Pro MC374 13"	2010	Administrasi	Hardware	2	2	1	5
278	DPTSI	DPTSI	Lap Top	6	Asus ZenBook Flip UX360CA-C4115T	2017	Programmer	Hardware	2	2	1	5
279	DPTSI	DPTSI	Lap Top	7	NoteBook Asus ZenBookAsus UX390UA-GS048T	2017	Programmer	Hardware	2	2	1	5
280	DPTSI	DPTSI	Lap Top	8	Apple Macbook MNYG2ID/A	2017	SI tester	Hardware	2	2	1	5
281	DPTSI	DPTSI	Note Book	2	HP Probook 4330s	2011	Network Administrasi	Hardware	2	2	1	5

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
282	DPTSI	DPTSI	Note Book	3	HP Probook 4330s	2011	Administrasi	Hardware	2	2	1	5
283	DPTSI	DPTSI	Note Book	4	HP Probook 4330s	2011	Administrasi	Hardware	2	2	1	5
284	DPTSI	DPTSI	Note Book	5	HP probook	2012	Network Administrasi	Hardware	2	2	1	5
285	DPTSI	DPTSI	Note Book	8	Lenovo	2012	Administrasi	Hardware	2	2	1	5
286	DPTSI	DPTSI	Note Book	10	Sony	2013	Network Administrasi	Hardware	2	2	1	5
287	DPTSI	DPTSI	Note Book	11	Lenovo	2013	Programmer	Hardware	2	2	1	5
288	DPTSI	DPTSI	Note Book	12	Lenovo	2013	Network Administrasi	Hardware	2	2	1	5
289	DPTSI	DPTSI	Note Book	13	HP/430	2014	Administrasi	Hardware	2	2	1	5
290	DPTSI	DPTSI	Note Book	14	Lenovo/G40	2014	Administrasi	Hardware	2	2	1	5
291	DPTSI	DPTSI	Note Book	15	Lenovo/G40	2014	Administrasi	Hardware	2	2	1	5
292	DPTSI	DPTSI	Note Book	16	Apple	2017	Administrasi	Hardware	2	2	1	5
293	DPTSI	DPTSI	Note Book	17	Lenovo	2017	Administrasi	Hardware	2	2	1	5
294	DPTSI	DPTSI	Note Book	18	Lenovo	2017	Administrasi	Hardware	2	2	1	5
295	DPTSI	DPTSI	Note Book	19	Asus A45 6UR putih	2017	Programmer	Hardware	2	2	1	5
296	DPTSI	DPTSI	Note Book	20	Asus A45 6UR putih	2017	Administrasi	Hardware	2	2	1	5

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
297	DPTSI	DPTSI	Note Book	21	Asus A45 6UR putih	2017	Administrasi	Hardware	2	2	1	5
298	DPTSI	DPTSI	Note Book	22	Asus A45 6UR putih	2017	Administrasi	Hardware	2	2	1	5
299	DPTSI	DPTSI	Note Book	23	Asus	2017	Administrasi	Hardware	2	2	1	5
300	DPTSI	DPTSI	Note Book	24	Asus	2017	Administrasi	Hardware	2	2	1	5
301	DPTSI	DPTSI	Note Book	25	Asus	2017	Administrasi	Hardware	2	2	1	5
302	DPTSI	DPTSI	Note Book	26	DELL Inspiron 14 (7460)	2017	Network Administrasi	Hardware	2	2	1	5
303	DPTSI	DPTSI	Note Book	27	DELL Inspiron 14 (7460)	2017	Network Administrasi	Hardware	2	2	1	5
304	DPTSI	DPTSI	Personal Computer	1	HP	2012	Administrasi	Hardware	2	2	1	5
305	DPTSI	DPTSI	P.C Unit	1	Intel NUC	2017	Pelatihan	Hardware	1	2	1	4
306	DPTSI	DPTSI	P.C Unit	2	Intel NUC	2017	Pelatihan	Hardware	1	2	1	4
307	DPTSI	DPTSI	P.C Unit	3	Intel NUC	2017	Pelatihan	Hardware	1	2	1	4
308	DPTSI	DPTSI	P.C Unit	4	Intel NUC	2017	Pelatihan	Hardware	1	2	1	4
309	DPTSI	DPTSI	P.C Unit	5	Intel NUC	2017	Pelatihan	Hardware	1	2	1	4
310	DPTSI	DPTSI	P.C Unit	6	Intel NUC	2017	Pelatihan	Hardware	1	2	1	4
311	DPTSI	DPTSI	P.C Unit	7	Intel NUC	2017	Pelatihan	Hardware	1	2	1	4

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
312	DPTSI	DPTSI	P.C Unit	8	Intel NUC	2017	Pelatihan	Hardware	1	2	1	4
313	DPTSI	DPTSI	P.C Unit	9	Intel NUC	2017	Pelatihan	Hardware	1	2	1	4
314	DPTSI	DPTSI	P.C Unit	10	Intel NUC	2017	Pelatihan	Hardware	1	2	1	4
315	DPTSI	DPTSI	P.C Unit	11	Intel NUC	2017	Pelatihan	Hardware	1	2	1	4
316	DPTSI	DPTSI	P.C Unit	12	Intel NUC	2017	Pelatihan	Hardware	1	2	1	4
317	DPTSI	DPTSI	P.C Unit	13	HP/Slimline	2015	Administrasi	Hardware	1	2	1	4
318	DPTSI	DPTSI	P.C Unit	21	HP Omni 200-5316L	2011	Administrasi	Hardware	2	2	1	5
319	DPTSI	DPTSI	P.C Unit	22	HP Pavilion	2013	Administrasi	Hardware	2	2	1	5
320	DPTSI	DPTSI	P.C Unit	23	HP Pavilion	2013	Administrasi	Hardware	2	2	1	5
321	DPTSI	DPTSI	P.C Unit	24	Simbadda	2014	Administrasi	Hardware	2	2	1	5
322	DPTSI	DPTSI	P.C Unit	25	Simbadda	2014	Administrasi	Hardware	2	2	1	5
323	DPTSI	DPTSI	P.C Unit	26	Simbadda	2014	Administrasi	Hardware	2	2	1	5
324	DPTSI	DPTSI	P.C Unit	27	HP Pro 4300SFF	2014	Programer	Hardware	2	2	1	5
325	DPTSI	DPTSI	P.C Unit	28	HP Pro 4300SFF	2014	Programer	Hardware	2	2	1	5
326	DPTSI	DPTSI	P.C Unit	29	hp	2016	Pelatihan	Hardware	2	2	1	5

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
327	DPTSI	DPTSI	P.C Unit	30	hp	2016	Pelatihan	Hardware	2	2	1	5
328	DPTSI	DPTSI	P.C Unit	31	hp	2016	Pelatihan	Hardware	2	2	1	5
329	DPTSI	DPTSI	P.C Unit	32	HP Pavilion 24-B121D	2017	Programer	Hardware	2	2	1	5
330	DPTSI	DPTSI	Personal Komputer Lainnya	1	-	2012	Programer	Hardware	2	2	1	5
331	DPTSI	DPTSI	Personal Komputer Lainnya	2	-	2012	Programer	Hardware	2	2	1	5
332	DPTSI	DPTSI	Personal Komputer Lainnya	3	-	2012	Programer	Hardware	2	2	1	5
333	DPTSI	DPTSI	Personal Komputer Lainnya	4	-	2012	Programer	Hardware	2	2	1	5
334	DPTSI	DPTSI	CPU (Peralatan Personal Komputer)	1	APPLE New MAC Mini	2017	Programer	Hardware	2	2	1	5
335	DPTSI	DPTSI	CPU (Peralatan Personal Komputer)	2	APPLE New MAC Mini	2017	Programer	Hardware	2	2	1	5
336	DPTSI	DPTSI	CPU (Peralatan Personal Komputer)	3	Apple	2018	Administrasi	Hardware	2	2	1	5
337	DPTSI	DPTSI	CPU (Peralatan Personal Komputer)	4	Apple	2018	Programer	Hardware	2	2	1	5
338	DPTSI	DPTSI	CPU (Peralatan Personal Komputer)	5	Apple	2018	Programer	Hardware	2	2	1	5
339	DPTSI	DPTSI	CPU (Peralatan Personal Komputer)	6	Apple	2018	Programer	Hardware	2	2	1	5
340	DPTSI	DPTSI	CPU (Peralatan Personal Komputer)	7	Apple	2018	Programer	Hardware	2	2	1	5
341	DPTSI	DPTSI	Printer (Peralatan Personal Komputer)	1	HP/M176N	2015		Hardware	1	2	1	4

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
342	DPTSI	DPTSI	Printer (Peralatan Personal Komputer)	10	HP LASERJET P2035N	2011		Hardware	1	2	1	4
343	DPTSI	DPTSI	Printer (Peralatan Personal Komputer)	12	Epson L100	2012		Hardware	1	2	1	4
344	DPTSI	DPTSI	Printer (Peralatan Personal Komputer)	14	HP Laserjet 1102	2013		Hardware	1	2	1	4
345	DPTSI	DPTSI	Printer (Peralatan Personal Komputer)	16	Brother PT-E300VP	2016		Hardware	1	2	1	4
346	DPTSI	DPTSI	Printer (Peralatan Personal Komputer)	17	HP/M-177FW	2016		Hardware	1	2	1	4
347	DPTSI	DPTSI	Printer (Peralatan Personal Komputer)	18	HP Laserjet M12w	2017		Hardware	1	2	1	4
348	DPTSI	DPTSI	Printer (Peralatan Personal Komputer)	19	Canon Pixma IP 110i	2017		Hardware	1	2	1	4
349	DPTSI	DPTSI	Printer (Peralatan Personal Komputer)	20	Printer Epson L120	2017		Hardware	1	2	1	4
350	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	1	APC BRI 100CI-AS	2010		Hardware	1	2	3	6
351	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	2	APC BRI 100CI-AS	2010		Hardware	1	2	3	6
352	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	3	UPS ONLINE	2010		Hardware	1	2	3	6
353	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	4	UPS ONLINE	2010		Hardware	1	2	3	6
354	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	5	UPS ONLINE	2010		Hardware	1	2	3	6
355	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	6	UPS ONLINE	2010		Hardware	1	2	3	6
356	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	7	UPS ONLINE	2010		Hardware	1	2	3	6

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
357	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	8	UPS ONLINE	2010		Hardware	1	2	3	6
358	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	9	UPS ONLINE	2010		Hardware	1	2	3	6
359	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	10	UPS	2012		Hardware	1	2	3	6
360	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	12	PASCAL Modular RM	2014		Hardware	1	2	3	6
361	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	13	APC Smart UPS C1000	2017		Hardware	1	2	3	6
362	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	14	APC Smart UPS C1000	2017		Hardware	1	2	3	6
363	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	15	APC Smart UPS C1000	2017		Hardware	1	2	3	6
364	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	16	APC Smart UPS C1000	2017		Hardware	1	2	3	6
365	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	17	APC Smart UPS C1000	2017		Hardware	1	2	3	6
366	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	18	APC Smart UPS C1000	2017		Hardware	1	2	3	6
367	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	19	APC Smart UPS C1000	2017		Hardware	1	2	3	6
368	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	20	APC Smart UPS C1000	2017		Hardware	1	2	3	6
369	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	21	APC Smart UPS C1000	2017		Hardware	1	2	3	6
370	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	22	APC Smart UPS C1000	2017		Hardware	1	2	3	6
371	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	23	APC Smart UPS C1000	2017		Hardware	1	2	3	6

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
372	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	24	APC	2018		Hardware	1	2	3	6
373	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	25	APC	2018		Hardware	1	2	3	6
374	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	26	APC	2018		Hardware	1	2	3	6
375	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	27	APC	2018		Hardware	1	2	3	6
376	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	28	APC	2018		Hardware	1	2	3	6
377	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	29	APC	2018		Hardware	1	2	3	6
378	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	30	APC	2018		Hardware	1	2	3	6
379	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	31	APC	2018		Hardware	1	2	3	6
380	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	32	APC	2018		Hardware	1	2	3	6
381	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	33	APC	2018		Hardware	1	2	3	6
382	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	34	APC	2018		Hardware	1	2	3	6
383	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	35	APC	2018		Hardware	1	2	3	6
384	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	36	APC	2018		Hardware	1	2	3	6
385	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	37	APC	2018		Hardware	1	2	3	6
386	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	38	APC	2018		Hardware	1	2	3	6

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
387	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	39	APC	2018		Hardware	1	2	3	6
388	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	40	APC	2018		Hardware	1	2	3	6
389	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	41	APC	2018		Hardware	1	2	3	6
390	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	42	APC	2018		Hardware	1	2	3	6
391	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	43	APC	2018		Hardware	1	2	3	6
392	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	44	APC	2018		Hardware	1	2	3	6
393	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	45	APC	2018		Hardware	1	2	3	6
394	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	46	APC	2018		Hardware	1	2	3	6
395	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	47	APC	2018		Hardware	1	2	3	6
396	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	48	APC	2018		Hardware	1	2	3	6
397	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	49	APC	2018		Hardware	1	2	3	6
398	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	50	APC	2018		Hardware	1	2	3	6
399	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	51	APC	2018		Hardware	1	2	3	6
400	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	52	APC	2018		Hardware	1	2	3	6
401	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	53	APC	2018		Hardware	1	2	3	6

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
402	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	54	APC	2018		Hardware	1	2	3	6
403	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	55	APC	2018		Hardware	1	2	3	6
404	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	56	APC	2018		Hardware	1	2	3	6
405	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	57	APC	2018		Hardware	1	2	3	6
406	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	58	APC	2018		Hardware	1	2	3	6
407	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	59	APC	2018		Hardware	1	2	3	6
408	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	60	APC	2018		Hardware	1	2	3	6
409	DPTSI	DPTSI	Uninterruptible Power Supply (UPS)	61	APC	2018		Hardware	1	2	3	6
410	DPTSI	DPTSI	Stabilizer/UPS	1	UPS Protekta	2009	UPS Server	Hardware	1	2	4	7
411	DPTSI	DPTSI	Uninterupted Power Supply (UPS)	1	PROLINK PRO 930 3000VA	2010		Hardware	1	2	3	6
412	DPTSI	DPTSI	Uninterupted Power Supply (UPS)	2	PROLINK PRO 930 3000VA	2010		Hardware	1	2	3	6
413	DPTSI	DPTSI	Uninterupted Power Supply (UPS)	3	UPS ICA RN 3200C	2011		Hardware	1	2	3	6
414	DPTSI	DPTSI	Uninterupted Power Supply (UPS)	4	UPS ICA RN 3200C	2011		Hardware	1	2	3	6
415	DPTSI	DPTSI	Uninterupted Power Supply (UPS)	5	UPS ICA RN 3200C	2011		Hardware	1	2	3	6
416	DPTSI	DPTSI	Uninterupted Power Supply (UPS)	6	UPS ICA RN 3200C	2011		Hardware	1	2	3	6

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
417	DPTSI	DPTSI	Uninterupted Power Supply (UPS)	7	Rackmounted TCL3300	2012	UPS Server	Hardware	1	2	4	7
418	DPTSI	DPTSI	Uninterupted Power Supply (UPS)	8	APC/UPS Smart	2013		Hardware	1	2	3	6
419	DPTSI	DPTSI	Uninterupted Power Supply (UPS)	9	APC/UPS Smart	2013		Hardware	1	2	3	6
420	DPTSI	DPTSI	Televisi	2	Samsung	2017	Monitoring	Hardware	2	2	2	6
421	DPTSI	DPTSI	Televisi	7	Sharp	2014	Monitoring	Hardware	2	2	2	6
422	DPTSI	DPTSI	Genset	1	CATERPILLAR ECW00427	2015		Hardware	1	2	4	7
423	DPTSI	DPTSI	Scanner (Universal Tester)	1	Canon DR 3060	2003		Hardware	1	2	1	4
424	DPTSI	DPTSI	Scanner (Universal Tester)	2	Canon DR 9080C	2003		Hardware	1	2	1	4
425	DPTSI	DPTSI	Scanner (Peralatan Mini Komputer)	1	NCS OPSCAN 5	2002		Hardware	1	2	1	4
426	DPTSI	DPTSI	Scanner (Peralatan Mini Komputer)	2	NCS OPSCAN 5	2002		Hardware	1	2	1	4
427	DPTSI	DPTSI	Scanner (Peralatan Mini Komputer)	3	NCS OPSCAN 5	2002		Hardware	1	2	1	4
428	DPTSI	DPTSI	Scanner (Peralatan Mini Komputer)	4	NCS OPSCAN 5	2002		Hardware	1	2	1	4
429	DPTSI	DPTSI	Scanner (Peralatan Mini Komputer)	5	NCS OPSCAN 5	2002		Hardware	1	2	1	4
430	DPTSI	DPTSI	Scanner (Peralatan Mini Komputer)	6	canon	2004		Hardware	1	2	1	4
431	DPTSI	DPTSI	Scanner (Peralatan Mini Komputer)	7	Intermec/SG20	2014		Hardware	1	2	1	4

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
432	DPTSI	DPTSI	Scanner (Peralatan Personal Komputer)	1	Fujitsu SP25	2015		Hardware	1	2	1	4
433	DPTSI	DPTSI	Scanner (Peralatan Personal Komputer)	3	Fujitsu	2014		Hardware	1	2	1	4
434	DPTSI	DPTSI	Scanner (Peralatan Personal Komputer)	8	Fujitsu ScanSnap S1300i	2017		Hardware	1	2	1	4
435	DPTSI	DPTSI	Scanner (Peralatan Personal Komputer)	9	Canon Scanner Lide 120	2017		Hardware	1	2	1	4
436	DPTSI	DPTSI	Pesawat Telephone	1	Panasonic KWI 505	2013		Hardware	1	2	1	4
437	DPTSI	DPTSI	Pesawat Telephone	2	Panasonic KWI 505	2013		Hardware	1	2	1	4
438	DPTSI	DPTSI	Digital Indicator LCD/Metric	1	Display key telp.	2010		Hardware	1	2	1	4
439	DPTSI	DPTSI	Telephone (PABX)	1	Panasonic	2015		Hardware	1	2	1	4
440	DPTSI	DPTSI	Telephone (PABX)	9	Panasonic KX-NS300	2016		Hardware	1	2	1	4
441	DPTSI	DPTSI	LCD Projector/Infocus	1	Infocus	2017		Hardware	1	2	1	4
442	DPTSI	DPTSI	LCD Projector/Infocus	2	Infocus	2017		Hardware	1	2	1	4
443	DPTSI	DPTSI	LCD Projector/Infocus	3	Infocus	2017		Hardware	1	2	1	4
444	DPTSI	DPTSI	LCD Projector/Infocus	7	Indisium	2013		Hardware	1	2	1	4
445	DPTSI	DPTSI	LCD Projector/Infocus	8	Philips Pico Pix ppx 4935	2017		Hardware	1	2	1	4
446	DPTSI	DPTSI	LCD Projector/Infocus	9	Philips Pico Pix ppx 4935	2017		Hardware	1	2	1	4

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
447	DPTSI	DPTSI	LCD Monitor	1	LCD Video Monitor	2012		Hardware	1	2	1	4
448	DPTSI	DPTSI	LCD Monitor	2	Samsung 32"	2013		Hardware	1	2	1	4
449	DPTSI	DPTSI	LCD Monitor	3	Samsung 32"	2013		Hardware	1	2	1	4
450	DPTSI	DPTSI	LCD Monitor	4	LG	2018		Hardware	1	2	1	4
451	DPTSI	DPTSI	LCD Monitor	5	LG	2018		Hardware	1	2	1	4
452	DPTSI	DPTSI	LCD Monitor	6	LG	2018		Hardware	1	2	1	4
453	DPTSI	DPTSI	LCD Monitor	7	LG	2018		Hardware	1	2	1	4
454	DPTSI	DPTSI	LCD Monitor	8	LG	2018		Hardware	1	2	1	4
455	DPTSI	DPTSI	Monitor	1	LG	2015		Hardware	1	2	1	4
456	DPTSI	DPTSI	Monitor	2	LG	2015		Hardware	1	2	1	4
457	DPTSI	DPTSI	Monitor	3	LCD Monitor LG	2009		Hardware	1	2	1	4
458	DPTSI	DPTSI	Monitor	4	Samsung 732 NW	2009		Hardware	1	2	1	4
459	DPTSI	DPTSI	Monitor	5	LCD Samsung732 NW	2009		Hardware	1	2	1	4
460	DPTSI	DPTSI	Monitor	6	Monitor LCD	2010		Hardware	1	2	1	4
461	DPTSI	DPTSI	Monitor	7	Monitor LCD	2010		Hardware	1	2	1	4

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
462	DPTSI	DPTSI	Monitor	8	LCD Monitotor	2010		Hardware	1	2	1	4
463	DPTSI	DPTSI	Monitor	9	LCD Monitotor	2010		Hardware	1	2	1	4
464	DPTSI	DPTSI	Monitor	10	LCD samsung	2009		Hardware	1	2	1	4
465	DPTSI	DPTSI	Monitor	11	LG 22MP58	2017		Hardware	1	2	1	4
466	DPTSI	DPTSI	Monitor	12	LG 22MP58	2017		Hardware	1	2	1	4
467	DPTSI	DPTSI	A.C. Split	1	Panasonic 2pk	2015	AC kantor	Hardware	2	2	1	5
468	DPTSI	DPTSI	A.C. Split	2	Panasonic	2015	AC kantor	Hardware	2	2	1	5
469	DPTSI	DPTSI	A.C. Split	21	Inverter 1 pk	2010	AC kantor	Hardware	2	2	1	5
470	DPTSI	DPTSI	A.C. Split	22	Type CS-D43DB4H5 (5 HP)	2010	Data Center AC	Hardware	2	3	4	9
471	DPTSI	DPTSI	A.C. Split	27	Panasonic	2013	Data Center AC	Hardware	2	3	4	9
472	DPTSI	DPTSI	A.C. Split	28	Panasonic	2014	Data Center AC	Hardware	2	3	4	9
473	DPTSI	DPTSI	A.C. Split	29	Panasonic	2014	Data Center AC	Hardware	2	3	4	9
474	DPTSI	DPTSI	A.C. Split	30	Panasonic 2PK	2016	AC kantor	Hardware	2	2	1	5
475	DPTSI	DPTSI	A.C. Split	31	Daikin STNE	2016	Data Center AC	Hardware	2	3	4	9
476	DPTSI	DPTSI	A.C. Split	32	Daikin STNE	2016	Data Center AC	Hardware	2	3	4	9

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
477	DPTSI	DPTSI	A.C. Split	33	Daikin STNE	2016	Data Center AC	Hardware	2	3	4	9
478	DPTSI	DPTSI	A.C. Split	34	Daikin STNE	2016	Data Center AC	Hardware	2	3	4	9
479	DPTSI	DPTSI	Air Conditioning (AC)	1	Panasonic	2012	AC kantor	Hardware	2	2	1	5
480	DPTSI	DPTSI	Air Conditioning (AC)	2	Panasonic	2012	AC kantor	Hardware	2	2	1	5
481	DPTSI	DPTSI	Tabung Pemadam Api	1	ECO	2002		Hardware	1	2	3	6
482	DPTSI	DPTSI	Tabung Pemadam Api	2	Appron AP -10 H	2002		Hardware	1	2	3	6
483	DPTSI	DPTSI	Tabung Pemadam Api	3	Worlmad	2002		Hardware	1	2	3	6
484	DPTSI	DPTSI	Tabung Pemadam Api	5		2002		Hardware	1	2	3	6
485	DPTSI	DPTSI	Tabung Pemadam Api	6	APPRON AP 6 H	2002		Hardware	1	2	3	6
486	DPTSI	DPTSI	Tabung Pemadam Api	7	APPRON AP 6 H	2002		Hardware	1	2	3	6
487	DPTSI	DPTSI	Tabung Pemadam Api	8	APPRON AP 6 H	2002		Hardware	1	2	3	6
488	DPTSI	DPTSI	Tabung Pemadam Api	9	APPRON AP 6 H	2002		Hardware	1	2	3	6
489	DPTSI	DPTSI	Tabung Pemadam Api	10		2002		Hardware	1	2	3	6
490	DPTSI	DPTSI	Tabung Pemadam Api	11	Appron AP 10 H	2002		Hardware	1	2	3	6
491	DPTSI	DPTSI	Tabung Pemadam Api	12	Swordsman	2002		Hardware	1	2	3	6

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
492	DPTSI	DPTSI	Tabung Pemadam Api	14	Appron AP 10 H	2002		Hardware	1	2	3	6
493	DPTSI	DPTSI	Tabung Pemadam Api	15	Appron AP 10 H	2002		Hardware	1	2	3	6
494	DPTSI	DPTSI	Tabung Pemadam Api	16	ECO	2002		Hardware	1	2	3	6
495	DPTSI	DPTSI	Tabung Pemadam Api	17	Blue -Benetron 5 kg	2018		Hardware	1	2	3	6
496	DPTSI	DPTSI	Tabung Pemadam Api	18	Blue -Benetron 5 kg	2018		Hardware	1	2	3	6
497	DPTSI	DPTSI	Tabung Pemadam Api	19	Blue -Benetron 5 kg	2018		Hardware	1	2	3	6
498	DPTSI	DPTSI	Tabung Pemadam Api	20	Blue -Benetron 5 kg	2018		Hardware	1	2	3	6
499	DPTSI	DPTSI	CCTV - Camera Control Television System	2	Hikvision	2018		Hardware	1	3	4	8
500	DPTSI	DPTSI	CCTV - Camera Control Television System	3	Hikvision	2018		Hardware	1	3	4	8
501	DPTSI	DPTSI	CCTV - Camera Control Television System	4	Hikvision	2018		Hardware	1	3	4	8
502	DPTSI	DPTSI	CCTV - Camera Control Television System	5	Hikvision	2018		Hardware	1	3	4	8
503	DPTSI	DPTSI	CCTV - Camera Control Television System	6	Hikvision	2018		Hardware	1	3	4	8
504	DPTSI	DPTSI	CCTV - Camera Control Television System	7	Hikvision	2018		Hardware	1	3	4	8
505	DPTSI	DPTSI	CCTV - Camera Control Television System	8	Hikvision	2018		Hardware	1	3	4	8
506	DPTSI	DPTSI	CCTV - Camera Control Television System	9	Hikvision	2018		Hardware	1	3	4	8

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
507	DPTSI	DPTSI	CCTV - Camera Control Television System	10	Hikvision	2018		Hardware	1	3	4	8
508	DPTSI	DPTSI	CCTV - Camera Control Television System	11	Hikvision	2018		Hardware	1	3	4	8
509	DPTSI	DPTSI	CCTV - Camera Control Television System	12	Hikvision	2018		Hardware	1	3	4	8
510	DPTSI	DPTSI	CCTV - Camera Control Television System	13	Hikvision	2018		Hardware	1	3	4	8
511	DPTSI	DPTSI	CCTV - Camera Control Television System	14	Hikvision	2018		Hardware	1	3	4	8
512	DPTSI	DPTSI	CCTV - Camera Control Television System	15	Hikvision	2018		Hardware	1	3	4	8
513	DPTSI	DPTSI	CCTV - Camera Control Television System	16	Hikvision	2018		Hardware	1	3	4	8
514	DPTSI	DPTSI	CCTV - Camera Control Television System	17	Hikvision	2018		Hardware	1	3	4	8
515	DPTSI	DPTSI	CCTV - Camera Control Television System	18	Hikvision	2018		Hardware	1	3	4	8
516	DPTSI	DPTSI	CCTV - Camera Control Television System	19	Hikvision	2018		Hardware	1	3	4	8
517	DPTSI	DPTSI	CCTV - Camera Control Television System	20	Hikvision	2018		Hardware	1	3	4	8
518	DPTSI	DPTSI	CCTV - Camera Control Television System	21	Hikvision	2018		Hardware	1	3	4	8
519	DPTSI	DPTSI	CCTV - Camera Control Television System	22	Hikvision	2018		Hardware	1	3	4	8
520	DPTSI	DPTSI	CCTV - Camera Control Television System	23	Hikvision	2018		Hardware	1	3	4	8
521	DPTSI	DPTSI	CCTV - Camera Control Television System	24	Hikvision	2018		Hardware	1	3	4	8

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
522	DPTSI	DPTSI	CCTV - Camera Control Television System	25	Hikvision	2018		Hardware	1	3	4	8
523	DPTSI	DPTSI	CCTV - Camera Control Television System	26	Hikvision	2018		Hardware	1	3	4	8
524	DPTSI	DPTSI	CCTV - Camera Control Television System	27	Hikvision	2018		Hardware	1	3	4	8
525	DPTSI	DPTSI	CCTV - Camera Control Television System	28	Hikvision	2018		Hardware	1	3	4	8
526	DPTSI	DPTSI	CCTV - Camera Control Television System	29	Hikvision	2018		Hardware	1	3	4	8
527	DPTSI	DPTSI	CCTV - Camera Control Television System	30	Hikvision	2018		Hardware	1	3	4	8
528	DPTSI	DPTSI	CCTV - Camera Control Television System	31	Hikvision	2018		Hardware	1	3	4	8
529	DPTSI	DPTSI	CCTV - Camera Control Television System	32	Hikvision	2018		Hardware	1	3	4	8
530	DPTSI	DPTSI	CCTV - Camera Control Television System	33	Hikvision	2018		Hardware	1	3	4	8
531	DPTSI	DPTSI	CCTV - Camera Control Television System	34	Hikvision	2018		Hardware	1	3	4	8
532	DPTSI	DPTSI	CCTV - Camera Control Television System	35	Hikvision	2018		Hardware	1	3	4	8
533	DPTSI	DPTSI	CCTV - Camera Control Television System	36	Hikvision	2018		Hardware	1	3	4	8
534	DPTSI	DPTSI	CCTV - Camera Control Television System	37	Hikvision	2018		Hardware	1	3	4	8
535	DPTSI	DPTSI	CCTV - Camera Control Television System	38	Hikvision	2018		Hardware	1	3	4	8
536	DPTSI	DPTSI	CCTV - Camera Control Television System	39	Hikvision	2018		Hardware	1	3	4	8

No	Organisasi & Proses Relevan		Detail Informasi Aset									
	Unit Operasi	Pemilik Proses	Nama Aset	NUP*	Merek / Type	Tahun Perolehan	Deskripsi Aset	Jenis Asset	NC	NI	NV	Asset Value
537	DPTSI	DPTSI	Camera Conference	1	Logitech	2018		Hardware	1	3	1	5
538	DPTSI	DPTSI	Camera Conference	2	Logitech	2018		Hardware	1	3	1	5
539	DPTSI	DPTSI	Alat Sidik Jari	1	FInger Prnt	2014	Pengaman Pintu	Hardware	3	4	4	11

Lampiran D

Penghitungan nilai ancaman pada aset kritis

Nama Aset Merk / Type Fungsi Tahun perolehan		SI Akademik	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
2	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
3	*Software failure* (kerusakan perangkat lunak)	Low	0.3
4	*User's error* (Kesalahan user)	Medium	0.4
5	*Administrator's error* (Kesalahan administrator)	Medium	0.4
6	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
7	*Malware diffusion* (pembauran Malware)	Medium	0.4
8	*Information leaks* (kebocoran informasi)	Low	0.1
9	*Information modification* (modifaki informasi)	Low	0.3
10	*Incorrect information entry* (salah memasukkan informasi)	Low	0.3
11	*Bug on software* (bug (kesalahan) software)	Low	0.3
12	*Defects in software maintenance or updating* (Cacat dalam pemeliharaan atau pembaruan perangkat lunak)	Low	0.1
13	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
14	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
15	*Malicious erasure of software configurations* (Penghapusan berbahaya konfigurasi perangkat lunak)	Low	0.1
16	*Abuse of access privileges* (Penyalahgunaan hak akses)	Low	0.3
17	*Unauthorized access* (Akses yang tidak sah)	Medium	0.4
18	*Traffic analysis* (Analisis lalu lintas)	Low	0.1
19	*Software manipulation* (Manipulasi perangkat lunak)	Low	0.2
20	*Denial of service* (Kegagalan layanan)	Low	0.1
		Jumlah	5.3
		NT	0.265

Nama Aset Merk / Type Fungsi Tahun perolehan		SIM Rencana Belanja Anggaran (SIM RBA)	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
2	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
3	*Software failure* (kerusakan perangkat lunak)	Low	0.3
4	*User's error* (Kesalahan user)	Medium	0.4
5	*Administrator's error* (Kesalahan administrator)	Medium	0.4
6	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
7	*Malware diffusion* (pembauran Malware)	Medium	0.4
8	*Information leaks* (kebocoran informasi)	Low	0.1
9	*Information modification* (modifaki informasi)	Low	0.3
10	*Incorrect information entry* (salah memasukkan informasi)	Low	0.3
11	*Bug on software* (bug (kesalahan) software)	Low	0.3
12	*Defects in software maintenance or updating* (Cacat dalam pemeliharaan atau pembaruan perangkat lunak)	Low	0.1
13	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
14	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
15	*Malicious erasure of software configurations* (Penghapusan berbahaya konfigurasi perangkat lunak)	Low	0.1
16	*Abuse of access privileges* (Penyalahgunaan hak akses)	Low	0.3
17	*Unauthorized access* (Akses yang tidak sah)	Medium	0.4
18	*Traffic analysis* (Analisis lalu lintas)	Low	0.1
19	*Software manipulation* (Manipulasi perangkat lunak)	Low	0.2
20	*Denial of service* (Kegagalan layanan)	Low	0.1
		Jumlah	5.3
		NT	0.265

Nama Aset Merk / Type Fungsi Tahun perolehan		SIM Keuangan	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
2	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
3	*Software failure* (kerusakan perangkat lunak)	Low	0.3
4	*User's error* (Kesalahan user)	Medium	0.4
5	*Administrator's error* (Kesalahan administrator)	Medium	0.4
6	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
7	*Malware diffusion* (pembauran Malware)	Medium	0.4
8	*Information leaks* (kebocoran informasi)	Low	0.1
9	*Information modification* (modifaki informasi)	Low	0.3
10	*Incorrect information entry* (salah memasukkan informasi)	Low	0.3
11	*Bug on software* (bug (kesalahan) software)	Low	0.3
12	*Defects in software maintenance or updating* (Cacat dalam pemeliharaan atau pembaruan perangkat lunak)	Low	0.1
13	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
14	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
15	*Malicious erasure of software configurations* (Penghapusan berbahaya konfigurasi perangkat lunak)	Low	0.1
16	*Abuse of access privileges* (Penyalahgunaan hak akses)	Low	0.3
17	*Unauthorized access* (Akses yang tidak sah)	Medium	0.4
18	*Traffic analysis* (Analisis lalu lintas)	Low	0.1
19	*Software manipulation* (Manipulasi perangkat lunak)	Low	0.2
20	*Denial of service* (Kegagalan layanan)	Low	0.1
		Jumlah	5.3
		NT	0.265

Nama Aset Merk / Type Fungsi Tahun perolehan		SI Monitoring Pendapatan ITS (SIMONDITS)	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
2	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
3	*Software failure* (kerusakan perangkat lunak)	Low	0.3
4	*User's error* (Kesalahan user)	Medium	0.4
5	*Administrator's error* (Kesalahan administrator)	Medium	0.4
6	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
7	*Malware diffusion* (pembauran Malware)	Medium	0.4
8	*Information leaks* (kebocoran informasi)	Low	0.1
9	*Information modification* (modifaki informasi)	Low	0.3

10	*Incorrect information entry* (salah memasukkan informasi)	Low	0.3
11	*Bug on software* (bug (kesalahan) software)	Low	0.3
12	*Defects in software maintenance or updating* (Cacat dalam pemeliharaan atau pembaruan perangkat lunak)	Low	0.1
13	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
14	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
15	*Malicious erasure of software configurations* (Penghapusan berbahaya konfigurasi perangkat lunak)	Low	0.1
16	*Abuse of access privileges* (Penyalahgunaan hak akses)	Low	0.3
17	*Unauthorized access* (Akses yang tidak sah)	Medium	0.4
18	*Traffic analysis* (Analisis lalu lintas)	Low	0.1
19	*Software manipulation* (Manipulasi perangkat lunak)	Low	0.2
20	*Denial of service* (Kegagalan layanan)	Low	0.1
		Jumlah	5.3
		NT	0.265

Nama Aset Merk / Type Fungsi Tahun perolehan		Host-to-host App	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
2	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
3	*Software failure* (kerusakan perangkat lunak)	Low	0.3
4	*User's error* (Kesalahan user)	Medium	0.4
5	*Administrator's error* (Kesalahan administrator)	Medium	0.4
6	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
7	*Malware diffusion* (pembauran Malware)	Medium	0.4
8	*Information leaks* (kebocoran informasi)	Low	0.1
9	*Information modification* (modifaki informasi)	Low	0.3
10	*Incorrect information entry* (salah memasukkan informasi)	Low	0.3
11	*Bug on software* (bug (kesalahan) software)	Low	0.3
12	*Defects in software maintenance or updating* (Cacat dalam pemeliharaan atau pembaruan perangkat lunak)	Low	0.1
13	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
14	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
15	*Malicious erasure of software configurations* (Penghapusan berbahaya konfigurasi perangkat lunak)	Low	0.1
16	*Abuse of access privileges* (Penyalahgunaan hak akses)	Low	0.3
17	*Unauthorized access* (Akses yang tidak sah)	Medium	0.4
18	*Traffic analysis* (Analisis lalu lintas)	Low	0.1
19	*Software manipulation* (Manipulasi perangkat lunak)	Low	0.2
20	*Denial of service* (Kegagalan layanan)	Low	0.1
		Jumlah	5.3
		NT	0.265

Nama Aset Merk / Type Fungsi Tahun perolehan		SIM Kepegawaian	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
2	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
3	*Software failure* (kerusakan perangkat lunak)	Low	0.3
4	*User's error* (Kesalahan user)	Medium	0.4
5	*Administrator's error* (Kesalahan administrator)	Medium	0.4
6	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
7	*Malware diffusion* (pembauran Malware)	Medium	0.4
8	*Information leaks* (kebocoran informasi)	Low	0.1
9	*Information modification* (modifaki informasi)	Low	0.3
10	*Incorrect information entry* (salah memasukkan informasi)	Low	0.3
11	*Bug on software* (bug (kesalahan) software)	Low	0.3
12	*Defects in software maintenance or updating* (Cacat dalam pemeliharaan atau pembaruan perangkat lunak)	Low	0.1
13	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
14	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
15	*Malicious erasure of software configurations* (Penghapusan berbahaya konfigurasi perangkat lunak)	Low	0.1
16	*Abuse of access privileges* (Penyalahgunaan hak akses)	Low	0.3
17	*Unauthorized access* (Akses yang tidak sah)	Medium	0.4
18	*Traffic analysis* (Analisis lalu lintas)	Low	0.1
19	*Software manipulation* (Manipulasi perangkat lunak)	Low	0.2
20	*Denial of service* (Kegagalan layanan)	Low	0.1
		Jumlah	5.3
		NT	0.265

Nama Aset Merk / Type Fungsi Tahun perolehan		Sistem Informasi Pelaporan Data	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
2	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
3	*Software failure* (kerusakan perangkat lunak)	Low	0.3
4	*User's error* (Kesalahan user)	Medium	0.4
5	*Administrator's error* (Kesalahan administrator)	Medium	0.4
6	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
7	*Malware diffusion* (pembauran Malware)	Medium	0.4
8	*Information leaks* (kebocoran informasi)	Low	0.1
9	*Information modification* (modifaki informasi)	Low	0.3

10	*Incorrect information entry* (salah memasukkan informasi)	Low	0.3
11	*Bug on software* (bug (kesalahan) software)	Low	0.3
12	*Defects in software maintenance or updating* (Cacat dalam pemeliharaan atau pembaruan perangkat lunak)	Low	0.1
13	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
14	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
15	*Malicious erasure of software configurations* (Penghapusan berbahaya konfigurasi perangkat lunak)	Low	0.1
16	*Abuse of access privileges* (Penyalahgunaan hak akses)	Low	0.3
17	*Unauthorized access* (Akses yang tidak sah)	Medium	0.4
18	*Traffic analysis* (Analisis lalu lintas)	Low	0.1
19	*Software manipulation* (Manipulasi perangkat lunak)	Low	0.2
20	*Denial of service* (Kegagalan layanan)	Low	0.1
		Jumlah	5.3
		NT	0.265

Nama Aset Merk / Type Fungsi Tahun perolehan		Executive Reporting	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
2	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
3	*Software failure* (kerusakan perangkat lunak)	Low	0.3
4	*User's error* (Kesalahan user)	Medium	0.4
5	*Administrator's error* (Kesalahan administrator)	Medium	0.4
6	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
7	*Malware diffusion* (pembauran Malware)	Medium	0.4
8	*Information leaks* (kebocoran informasi)	Low	0.1
9	*Information modification* (modifaki informasi)	Low	0.3
10	*Incorrect information entry* (salah memasukkan informasi)	Low	0.3
11	*Bug on software* (bug (kesalahan) software)	Low	0.3
12	*Defects in software maintenance or updating* (Cacat dalam pemeliharaan atau pembaruan perangkat lunak)	Low	0.1
13	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
14	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
15	*Malicious erasure of software configurations* (Penghapusan berbahaya konfigurasi perangkat lunak)	Low	0.1
16	*Abuse of access privileges* (Penyalahgunaan hak akses)	Low	0.3
17	*Unauthorized access* (Akses yang tidak sah)	Medium	0.4
18	*Traffic analysis* (Analisis lalu lintas)	Low	0.1
19	*Software manipulation* (Manipulasi perangkat lunak)	Low	0.2
20	*Denial of service* (Kegagalan layanan)	Low	0.1
		Jumlah	5.3
		NT	0.265

Nama Aset Merk / Type Fungsi Tahun perolehan		Sistem Informasi Pelaporan Data	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
2	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
3	*Software failure* (kerusakan perangkat lunak)	Low	0.3
4	*User's error* (Kesalahan user)	Medium	0.4
5	*Administrator's error* (Kesalahan administrator)	Medium	0.4
6	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
7	*Malware diffusion* (pembauran Malware)	Medium	0.4
8	*Information leaks* (kebocoran informasi)	Low	0.1
9	*Information modification* (modifaki informasi)	Low	0.3
10	*Incorrect information entry* (salah memasukkan informasi)	Low	0.3
11	*Bug on software* (bug (kesalahan) software)	Low	0.3
12	*Defects in software maintenance or updating* (Cacat dalam pemeliharaan atau pembaruan perangkat lunak)	Low	0.1
13	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
14	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
15	*Malicious erasure of software configurations* (Penghapusan berbahaya konfigurasi perangkat lunak)	Low	0.1
16	*Abuse of access privileges* (Penyalahgunaan hak akses)	Low	0.3
17	*Unauthorized access* (Akses yang tidak sah)	Medium	0.4
18	*Traffic analysis* (Analisis lalu lintas)	Low	0.1
19	*Software manipulation* (Manipulasi perangkat lunak)	Low	0.2
20	*Denial of service* (Kegagalan layanan)	Low	0.1
		Jumlah	5.3
		NT	0.265

Nama Aset Merk / Type Fungsi Tahun perolehan		Single Sign On (SSO) App	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
2	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
3	*Software failure* (kerusakan perangkat lunak)	Low	0.3
4	*User's error* (Kesalahan user)	Medium	0.4
5	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
6	*Malware diffusion* (pembauran Malware)	Medium	0.4
7	*Information leaks* (kebocoran informasi)	Low	0.1
8	*Bug on software* (bug (kesalahan) software)	Low	0.3
9	*Defects in software maintenance or updating* (Cacat dalam pemeliharaan atau pembaruan perangkat lunak)	Low	0.1

10	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
11	*Malicious erasure of software configurations* (Penghapusan berbahaya konfigurasi perangkat lunak)	Low	0.1
12	*Abuse of access privileges* (Penyalahgunaan hak akses)	Low	0.3
13	*Unauthorized access* (Akses yang tidak sah)	Medium	0.4
14	*Traffic analysis* (Analisis lalu lintas)	Low	0.1
15	*Software manipulation* (Manipulasi perangkat lunak)	Low	0.2
16	*Denial of service* (Kegagalan layanan)	Low	0.1
		Jumlah	4.1
		NT	0.25625

Nama Aset Merk / Type Fungsi Tahun perolehan		Modulas Monitoring System Network Backbone 2009	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
2	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
3	*Media degradation* (Degradasi Media)	High	0.8
4	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
5	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
6	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
		Jumlah	2.2
		NT	0.366666667

Nama Aset Merk / Type Fungsi Tahun perolehan		Fiber Optic Operating GE Network Backbone 2010	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
2	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
3	*Media degradation* (Degradasi Media)	High	0.8
4	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
5	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
6	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
		Jumlah	2.2
		NT	0.366666667

Nama Aset Merk / Type Fungsi Tahun perolehan		Interface Network CISCO Network Backbone 2010	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
2	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
3	*Media degradation* (Degradasi Media)	High	0.8
4	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
5	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
6	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
		Jumlah	2.2
		NT	0.366666667

Nama Aset Merk / Type Fungsi Tahun perolehan		Interface Network CISCO Network Backbone 2010	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
2	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
3	*Media degradation* (Degradasi Media)	High	0.8
4	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
5	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
6	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
		Jumlah	2.2
		NT	0.366666667

Nama Aset Merk / Type Fungsi Tahun perolehan		Paralel Control Network CISCO Network Backbone 2010	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
2	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
3	*Media degradation* (Degradasi Media)	High	0.8
4	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
5	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
6	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
		Jumlah	2.2
		NT	0.366666667

Nama Aset		Server	
Merk / Type		HPE DL580 Gen9 CTO SVR	
Fungsi		OLTP server dan OLAP Server	
Tahun perolehan		2017	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Short Circuit* (Konsleting*)*	Medium	0.4
2	*Power failure* (Kerusakan sumber listrik*)*	Low	0.1
3	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
4	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
5	*Software failure* (kerusakan perangkat lunak)	Low	0.3
6	*HVAC failure* (Kerusakan HVAC)	Low	0.1
7	*Administrator's error* (Kesalahan administrator)	Medium	0.4
8	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
9	*Malware diffusion* (pembauran Malware)	Medium	0.4
10	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
11	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
12	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
13	*Saturation of the network caused by a worm* (Kejenuhan jaringan disebabkan oleh worm)	Medium	0.4
14	*Hardware misuse* (Penyalahgunaan perangkat keras)	Low	0.1
15	*Denial of service* (Kegagalan layanan)	Low	0.1
		Jumlah	3.9
		NT	0.26

Nama Aset		Server	
Merk / Type		HPE DL380 Gen9 CTO Derver	
Fungsi		VMWare 65 Server	
Tahun perolehan		2017	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Short Circuit* (Konsleting*)*	Medium	0.4
2	*Power failure* (Kerusakan sumber listrik*)*	Low	0.1
3	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
4	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
5	*Software failure* (kerusakan perangkat lunak)	Low	0.3
6	*HVAC failure* (Kerusakan HVAC)	Low	0.1
7	*Administrator's error* (Kesalahan administrator)	Medium	0.4
8	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
9	*Malware diffusion* (pembauran Malware)	Medium	0.4
10	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
11	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
12	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
13	*Saturation of the network caused by a worm* (Kejenuhan jaringan disebabkan oleh worm)	Medium	0.4

14	*Hardware misuse* (Penyalahgunaan perangkat keras)	Low	0.1
15	*Denial of service* (Kegagalan layanan)	Low	0.1
		Jumlah	3.9
		NT	0.26

Nama Aset		Server	
Merk / Type		HP / PROLIANT ML150	
Fungsi		Server Aplikasi Unit	
Tahun perolehan		2005	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Short Circuit* (Konsleting*)*	Medium	0.4
2	*Power failure* (Kerusakan sumber listrik*)*	Low	0.1
3	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
4	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
5	*Software failure* (kerusakan perangkat lunak)	Low	0.3
6	*Media degradation* (Degradasi Media)	High	0.8
7	*HVAC failure* (Kerusakan HVAC)	Low	0.1
8	*Administrator's error* (Kesalahan administrator)	Medium	0.4
9	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
10	*Malware diffusion* (pembauran Malware)	Medium	0.4
11	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
12	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
13	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
14	*Saturation of the network caused by a worm* (Kejenuhan jaringan disebabkan oleh worm)	Medium	0.4
15	*Hardware misuse* (Penyalahgunaan perangkat keras)	Low	0.1
16	*Denial of service* (Kegagalan layanan)	Low	0.1
		Jumlah	4.7
		NT	0.29375

Nama Aset		Server	
Merk / Type		Advance Server SUN X4100	
Fungsi		Data Center	
Tahun perolehan		2009	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Short Circuit* (Konsleting*)*	Medium	0.4
2	*Power failure* (Kerusakan sumber listrik*)*	Low	0.1
3	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
4	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
5	*Software failure* (kerusakan perangkat lunak)	Low	0.3
6	*Media degradation* (Degradasi Media)	High	0.8
7	*HVAC failure* (Kerusakan HVAC)	Low	0.1
8	*Administrator's error* (Kesalahan administrator)	Medium	0.4
9	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
10	*Malware diffusion* (pembauran Malware)	Medium	0.4

11	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
12	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
13	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
14	*Saturation of the network caused by a worm* (Kejenuhan jaringan disebabkan oleh worm)	Medium	0.4
15	*Hardware misuse* (Penyalahgunaan perangkat keras)	Low	0.1
16	*Denial of service* (Kegagalan layanan)	Low	0.1
		Jumlah	4.7
		NT	0.29375

Nama Aset Merk / Type Fungsi Tahun perolehan		Wireless Access Point Cisco/AIR-CAP2702I-F Distributor Wireless AP 2016	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Short Circuit* (Konsleting*)*	Medium	0.4
2	*Power failure* (Kerusakan sumber listrik*)*	Low	0.1
3	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
4	*Administrator's error* (Kesalahan administrator)	Medium	0.4
5	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
6	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
7	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
8	*Denial of service* (Kegagalan layanan)	Low	0.1
		Jumlah	2
		NT	0.25

Nama Aset Merk / Type Fungsi Tahun perolehan		Wireless Access Point CISCO Aironet 1852E Distributor Wireless AP 2017	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Short Circuit* (Konsleting*)*	Medium	0.4
2	*Power failure* (Kerusakan sumber listrik*)*	Low	0.1
3	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
4	*Administrator's error* (Kesalahan administrator)	Medium	0.4
5	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
6	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
7	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
8	*Denial of service* (Kegagalan layanan)	Low	0.1
		Jumlah	2
		NT	0.25

Nama Aset Merk / Type Fungsi Tahun perolehan		Firewall Barracuda 641 ADC Network Firewall 2017	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Short Circuit* (Konsleting*)*	Medium	0.4
2	*Power failure* (Kerusakan sumber listrik*)*	Low	0.1
3	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
4	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
5	*Administrator's error* (Kesalahan administrator)	Medium	0.4
6	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
7	*[Re]-routing error* (kesalahan routing data)	Low	0.1
8	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
9	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
10	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
11	*Hardware misuse* (Penyalahgunaan perangkat keras)	Low	0.1
12	*Network misuse* (Penyalahgunaan jaringan)	Low	0.1
13	*Unauthorized access* (Akses yang tidak sah)	Medium	0.4
		Jumlah	3.2
		NT	0.246153846

Nama Aset Merk / Type Fungsi Tahun perolehan		Firewall Firewall Cisco ASA 5585-X Network Firewall 2011	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Short Circuit* (Konsleting*)*	Medium	0.4
2	*Power failure* (Kerusakan sumber listrik*)*	Low	0.1
3	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
4	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
5	*Administrator's error* (Kesalahan administrator)	Medium	0.4
6	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
7	*[Re]-routing error* (kesalahan routing data)	Low	0.1
8	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
9	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
10	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
11	*Hardware misuse* (Penyalahgunaan perangkat keras)	Low	0.1
12	*Network misuse* (Penyalahgunaan jaringan)	Low	0.1
13	*Unauthorized access* (Akses yang tidak sah)	Medium	0.4
		Jumlah	3.2
		NT	0.246153846

Nama Aset Merk / Type Fungsi Tahun perolehan		Router Gigabit Router Cisco 3945 Main Router 2011	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Short Circuit* (Konsleting*)*	Medium	0.4
2	*Power failure* (Kerusakan sumber listrik*)*	Low	0.1
3	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
4	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
5	*Administrator's error* (Kesalahan administrator)	Medium	0.4
6	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
7	*[Re]-routing error* (kesalahan routing data)	Low	0.1
8	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
9	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
10	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
11	*Hardware misuse* (Penyalahgunaan perangkat keras)	Low	0.1
12	*Network misuse* (Penyalahgunaan jaringan)	Low	0.1
		Jumlah	2.8
		NT	0.233333333

Nama Aset Merk / Type Fungsi Tahun perolehan		Router CISCO 7606 S Core Router 2012	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Short Circuit* (Konsleting*)*	Medium	0.4
2	*Power failure* (Kerusakan sumber listrik*)*	Low	0.1
3	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
4	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
5	*Administrator's error* (Kesalahan administrator)	Medium	0.4
6	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
7	*[Re]-routing error* (kesalahan routing data)	Low	0.1
8	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
9	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
10	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
11	*Hardware misuse* (Penyalahgunaan perangkat keras)	Low	0.1
12	*Network misuse* (Penyalahgunaan jaringan)	Low	0.1
		Jumlah	2.8
		NT	0.233333333

Nama Aset Merk / Type Fungsi Tahun perolehan		Auto Switch/Data Switch CISCO 4900 Access Switch 2010	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Short Circuit* (Konsleting*)*	Medium	0.4
2	*Power failure* (Kerusakan sumber listrik*)*	Low	0.1
3	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
4	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
5	*Administrator's error* (Kesalahan administrator)	Medium	0.4
6	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
7	*[Re]-routing error* (kesalahan routing data)	Low	0.1
8	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
9	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
10	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
11	*Hardware misuse* (Penyalahgunaan perangkat keras)	Low	0.1
12	*Network misuse* (Penyalahgunaan jaringan)	Low	0.1
		Jumlah	2.8
		NT	0.233333333

Nama Aset Merk / Type Fungsi Tahun perolehan		Auto Switch/Data Switch CISCO 3560 Access Switch 2010	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Short Circuit* (Konsleting*)*	Medium	0.4
2	*Power failure* (Kerusakan sumber listrik*)*	Low	0.1
3	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
4	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
5	*Administrator's error* (Kesalahan administrator)	Medium	0.4
6	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
7	*[Re]-routing error* (kesalahan routing data)	Low	0.1
8	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
9	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
10	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
11	*Hardware misuse* (Penyalahgunaan perangkat keras)	Low	0.1
12	*Network misuse* (Penyalahgunaan jaringan)	Low	0.1
		Jumlah	2.8
		NT	0.233333333

Nama Aset Merk / Type Fungsi Tahun perolehan		Switch Database Data Switch Access Switch 2017	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Short Circuit* (Konsleting*)*	Medium	0.4
2	*Power failure* (Kerusakan sumber listrik*)*	Low	0.1
3	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
4	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
5	*Administrator's error* (Kesalahan administrator)	Medium	0.4
6	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
7	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
8	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
9	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
10	*Hardware misuse* (Penyalahgunaan perangkat keras)	Low	0.1
11	*Network misuse* (Penyalahgunaan jaringan)	Low	0.1
		Jumlah	2.7
		NT	0.245454545

Nama Aset Merk / Type Fungsi Tahun perolehan		Switch Cisco Catalyst 3560X 24 Port Access Switch 2011	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Short Circuit* (Konsleting*)*	Medium	0.4
2	*Power failure* (Kerusakan sumber listrik*)*	Low	0.1
3	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
4	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
5	*Administrator's error* (Kesalahan administrator)	Medium	0.4
6	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
7	*[Re]-routing error* (kesalahan routing data)	Low	0.1
8	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
9	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
10	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
11	*Hardware misuse* (Penyalahgunaan perangkat keras)	Low	0.1
12	*Network misuse* (Penyalahgunaan jaringan)	Low	0.1
		Jumlah	2.8
		NT	0.233333333

Nama Aset	Storage Modul Disk (Peralatan Mainframe)		
Merk / Type	SAN/Storage		
Fungsi	Data Centre		
Tahun perolehan	2012		
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Short Circuit* (Konsleting*)*	Medium	0.4
2	*Power failure* (Kerusakan sumber listrik*)*	Low	0.1
3	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
4	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
5	*Media degradation* (Degradasi Media)	High	0.8
6	*Administrator's error* (Kesalahan administrator)	Medium	0.4
7	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
8	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
9	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
10	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
11	*Unauthorized access* (Akses yang tidak sah)	Medium	0.4
12	*Denial of service* (Kegagalan layanan)	Low	0.1
		Jumlah	3.8
		NT	0.316666667

Nama Aset	Storage Modul Disk (Peralatan Mainframe)		
Merk / Type	Hitachi/HUS110		
Fungsi	Data Centre		
Tahun perolehan	2014		
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Short Circuit* (Konsleting*)*	Medium	0.4
2	*Power failure* (Kerusakan sumber listrik*)*	Low	0.1
3	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
4	*Network failure* (kerusakan jaringan komputer*)*	Medium	0.4
5	*Media degradation* (Degradasi Media)	High	0.8
6	*Administrator's error* (Kesalahan administrator)	Medium	0.4
7	*Configuration Error* (Kesalahan konfigurasi)	Low	0.3
8	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
9	*Defects in network maintenance* (Cacat dalam pemeliharaan jaringan)	Low	0.2
10	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
11	*Unauthorized access* (Akses yang tidak sah)	Medium	0.4
12	*Denial of service* (Kegagalan layanan)	Low	0.1
		Jumlah	3.8
		NT	0.316666667

Nama Aset Merk / Type Fungsi Tahun perolehan		Stabilizer/UPS UPS Protekta UPS Server 2009	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Short Circuit* (Konsleting*)*	Medium	0.4
2	*Power failure* (Kerusakan sumber listrik*)*	Low	0.1
3	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
4	*Media degradation* (Degradasi Media)	High	0.8
5	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
6	*System failure due to exhaustion of resources* (Kegagalan sistem karena kehabisan sumber daya)	Low	0.1
7	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
		Jumlah	2.1
		NT	0.3

Nama Aset Merk / Type Fungsi Tahun perolehan		Uninterupted Power Supply (UPS) Rackmounted TCL3300 UPS Server 2012	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Short Circuit* (Konsleting*)*	Medium	0.4
2	*Power failure* (Kerusakan sumber listrik*)*	Low	0.1
3	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
4	*Media degradation* (Degradasi Media)	High	0.8
5	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
6	*System failure due to exhaustion of resources* (Kegagalan sistem karena kehabisan sumber daya)	Low	0.1
7	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
		Jumlah	2.1
		NT	0.3

Nama Aset		A.C. Split	
Merk / Type		Type CS-D43DB4H5 (5 HP)	
Fungsi		Data Center AC	
Tahun perolehan		2010	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Short Circuit* (Konsleting*)*	Medium	0.4
2	*Power failure* (Kerusakan sumber listrik*)*	Low	0.1
3	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
4	*Media degradation* (Degradasi Media)	High	0.8
5	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
6	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
		Jumlah	2
		NT	0.333333333

Nama Aset		Daikin STNE	
Merk / Type		Type CS-D43DB4H5 (5 HP)	
Fungsi		Data Center AC	
Tahun perolehan		2016	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Short Circuit* (Konsleting*)*	Medium	0.4
2	*Power failure* (Kerusakan sumber listrik*)*	Low	0.1
3	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
4	*Media degradation* (Degradasi Media)	High	0.8
5	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
6	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
		Jumlah	2
		NT	0.333333333

Nama Aset		CCTV - Camera Control Television System	
Merk / Type		Hikvision	
Fungsi		Kamera Pengaman	
Tahun perolehan		2018	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Short Circuit* (Konsleting*)*	Medium	0.4
2	*Power failure* (Kerusakan sumber listrik*)*	Low	0.1
3	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
4	*Media degradation* (Degradasi Media)	High	0.8
5	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
6	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
		Jumlah	2
		NT	0.333333333

Nama Aset Merk / Type Fungsi Tahun perolehan		Alat Sidik Jari FInger Prnt Pengaman Pintu 2014	
No.	Jenis ancaman	Probabilitas	Rerata Probabilitas
1	*Short Circuit* (Konsleting*)*	Medium	0.4
2	*Power failure* (Kerusakan sumber listrik*)*	Low	0.1
3	*Hardware failure* (kerusakan perangkat keras*)*	Medium	0.4
4	*Media degradation* (Degradasi Media)	High	0.8
5	*Defects in hardware maintenance* (Cacat dalam pemeliharaan perangkat keras)	Low	0.2
6	*Hardware theft* (Pencurian perangkat keras)	Low	0.1
		Jumlah	2
		NT	0.333333333

LAMPIRAN E

Draft Kebijakan Keamanan Informasi

KEBIJAKAN KEAMANAN INFORMASI

INSTITUT TEKNOLOGI SEPULUH NOPEMBER

SURABAYA

Nomor Dokumen	: ……..
Revisi	: ……..
Tanggal Terbit	: ……..

LEMBAR PERSETUJUAN

Disiapkan Oleh :

1…….. Tanda Tangan: ……..

2…….. Tanda Tangan: ……..

Diperiksa Oleh:

1…….. Tanda Tangan: ……..

2…….. Tanda Tangan: ……..

Disetujui Oleh:

1…….. Tanda Tangan: ……..

2…….. Tanda Tangan: ……..

DAFTAR PERUBAHAN DOKUMEN

Rev	Tanggal	Uraian	Penanggungjawab
0.0	Edisi Awal		

[Halaman ini sengaja dikosongkan]

1. Pendahuluan

Informasi merupakan aset yang sangat penting bagi Instansi penyelenggara layanan publik dan karenanya perlu dilindungi dari ancaman yang dapat mengganggu kelangsungan bisnisnya. Penggunaan fasilitas teknologi informasi selain memudahkan proses pekerjaan juga mengandung risiko bila tidak digunakan dan dikelola dengan tepat. Oleh karena itu, penggunaan teknologi informasi harus dikelola sedemikian rupa sehingga memberi manfaat sebesarbesarnya dengan kemungkinan risiko yang rendah. Kebijakan ini didokumentasikan sebagai panduan untuk melindungi informasi dari ancaman keamanan informasi yang meliputi kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) dan mengurangi dampak dari terjadinya insiden keamanan.

2. Tujuan

(1) Melindungi aset informasi Institut Teknologi Sepuluh Nopember dalam rangka penyelenggara layanan publik dari segala bentuk ancaman, baik eksternal maupun internal, sengaja atau tidak.

(2) Sebagai referensi kepada seluruh komponen pelaksana keamanan informasi TI Institut Teknologi Sepuluh Nopember dalam menyusun dan menetapkan prosedur operasional agar terjadi keselarasan pada tataran strategis dan operasional.

3. Ruang Lingkup

(1) Kebijakan Keamanan Informasi ini diberlakukan secara menyeluruh di seluruh komponen organisasi Institut Teknologi Sepuluh Nopember.

(2) Kebijakan Keamanan Informasi ini mengatur Tata Kelola keamanan informasi dan Management Keamanan informasi.

4. Referensi

(1) Standar ISO 27001:2013

(2) Peraturan Menteri Komunikasi Dan Informatika, Nomor: 41/PER/MEN.KOMINFO/11/2007 tentang Panduan Tata Kelola Teknologi Informasi dan Komunikasi Nasional.

(3) Keputusan Rektor no.10 Tahun 2016, tentang Organisasi dan Tata Kerja ITS.

5. Kebijakan Umum Keamanan Informasi

(1) Kebijakan keamanan informasi di Institut Teknologi Sepuluh Nopember menjadi panduan dan pedoman untuk melaksanakan kegiatan yang ada hubungannya dengan keamanan informasi di Institut ini.

(2) Kebijakan keamanan informasi harus disosialisasikan dan dikomunikasikan ke seluruh Dosen, Pegawai, Mahasiswa dan pihak ketiga

terkait melalui media komunikasi yang ada agar dipahami dengan mudah dan dipatuhi.

(3) Seluruh kelemahan keamanan informasi yang berpotensi atau telah mengakibatkan gangguan penggunaan TI harus segera dilaporkan ke penanggung jawab TI terkait.

(4) Setiap pelanggaran terhadap kebijakan ini yang relevan dapat dikenai sanksi atau tindakan disiplin sesuai peraturan yang berlaku.

(5) Setiap detail teknis pelaksanaan tata kelola keamanan informasi yang tidak tercantum dalam kebijakan keamanan ini diatur dengan prosedur dan petunjuk pelaksanaan.

(6) Perubahan atau penambahan pada kebijakan informasi harus disetujui oleh bagian yang berkaitan, dan bisa dipertanggungjawabkan.

6. Peran dan Tanggung Jawab Organisasi Keamanan Informasi

(1) Rektor mendelegasikan sebagian tanggung jawab Tata Kelola TI di Institut Teknologi Sepuluh Nopember kepada DPTSI yang ditetapkan melalui Surat Keputusan Rektor no.10 Tahun 2016, tentang Organisasi dan Tata Kerja ITS.

(2) DPTSI bertanggung jawab untuk memberikan rekomendasi strategis kepada Rektor atas hasil Evaluasi, Arahan dan Pengawasan Teknologi Informasi di ITS.

(3) Peran Organisasi Keamanan Informasi di Institut Teknologi Sepuluh Nopember adalah:
   a. Mencegah terjadinya kehilangan atau kerusakan informasi di ITS
   b. Mengurangi risiko dari ancaman dari luar yang berkaitan dengan informasi di ITS.
   c. Menjaga informasi yang ada tidak digunakan secara sembarangan oleh pihak yang tidak
   d. Berwenang.

(4) Struktur organisasi keamanan informasi dibentuk atas dasar kepentingan realisasi Peran Strategis keamanan informasi di ITS.

(5) Rektor menetapkan Kebijakan Keamanan Informasi Institut melalui Surat Keputusan Rektor, dan melaksanakan peninjauna ulang secara berkala agar kebijakan sesuai dengan situasi dan kondisi terkini.

7. Manajemen Aset

(1) Seluruh aset yang berkaitan dengan keamanan informasi harus tercatat dalam SIM e-Aset, diberi label penanda dan diawasi pada jangka waktu yang ditentukan, baik aset fisik maupun non fisik.

(2) Setiap Seksi di DPTSI harus melakukan analisa resiko setiap asset sesuai dengan prosedur yang tertulis di Pedoman Instruksi Kerja.

(3) Setiap perubahan dokumen daftar asset dan analisa resiko harus di tandatangani oleh kepala seksi , kasubdit dan Direktur.
(4) DPTSI harus membuat pedoman tentang klasifikasi keamanan informasi, tata keloka informasi, penghancuran informasi.
(5) Setiap pemindahan aset fisik harus dilengkapi dengan berita acara perpindahan aset yang ditandatangi oleh kepala seksi dan kasubdit.
(6) Setiap Seksi harus membuat prosedur pemakaian aset dan tata cara perawatan aset.
(7) Peralatan sumber daya informasi institut harus ditempatkan dengan aman dan terlindung untuk menurunkan risiko terhadap ancaman lingkungan dan bahaya serta peluang dari akses yang tidak memiliki wewenang, serta terlindungi dari kegagalan suplai sumber daya energi dan gangguan lainnya yang diakibatkan kegagalan utility pendukung.
(8) Penggunaan peralatan sumber daya informasi institut di luar area kerja lingkungan institut harus mendapatkan persetujuan pihak atasan atau manajemen yang terkait dan tercatat.
(9) Setiap kerusakan aset harus dilaporkan kepada petugas Aset dan dicatat dalam berita acara kerusakan aset.
(10) Setiap kejadian kehilangan dan perbaikan informasi dan perangkat informasi harus tercatat pada dokumen kejadian perkara.
(11) Penggantian aset karena kerusakan haruslah dengan spesifikasi aset yang sesuai atau lebih tinggi dari aset yang rusak.
(12) Perangkat aset Informasi yang berusia lebih dari 4 tahun tidak boleh digunakan sebagai layanan yang bersifat kritis.
(13) Penghapusan aset dilakukan sesuai dengan aturan pemerintah dan dipastikan tidak ada informasi yang masih tersimpan didalamnya.

8. Kontrol Akses

(1) Setiap pengguna yang akan mengakses seluruh sistem informasi dan layanan informasi lainnya harus terdaftar dan mendapat izin akses dari unit kerja DPTSI dan atau unit kerja pemilik informasi.
(2) Hak akses akan diberikan kepada pengguna dalam bentuk user-id yang unik serta password yang kuat oleh unit kerja Teknologi dan Keamanan informasi dan atau unit kerja pemilik informasi.
(3) Pengguna yang mendapat hak akses harus melakukan penggunaan password yang kuat, yaitu kumpulan karakter yang terdiri dari huruf, angka dan symbol dengan minimal jumlah 8 karakter serta pembatasan umur password maksimal 120 hari, untuk menghindari pembobolan password oleh pihak yang tidak memiliki otoritas.
(4) Setiap pengguna jaringan harus terdaftar dan mendapat izin akses dari DPTSI.
(5) Unit kerja DPTSI harus melakukan pengendalian koneksi pada layanan jaringan melalui:
    a. Pemisahan jaringan harus berdasarkan grup layanan informasi, kelompok pengguna atau unit kerja serta lokasi dengan menerapkan segmentasi jaringan.

b. Harus dilakukan pembatasan jumlah akses dan waktu akses terhadap layanan jaringan yang di-share
c. Pengendalian harus di setiap jalur jaringan terhadap setiap koneksi komputer dan alur informasi, sehingga tidak terjadi pelanggaran hak akses terhadap aplikasi bisnis

(6) Pembatasan akses informasi dan fungsi-fungsi harus terdapat pada sistem aplikasi, merupakan wewenang dan tanggung jawab DPTSI.
(7) Setiap user password yang dialihkan ke orang lain harus menggunakan surat kuasa bermaterai dengan batas maksimal penggunaan selama 30 hari, dan penerima kuasa bertanggung jawab penuh atas penggunaan user dan password tersebut.
(8) Pemilik user password harus melakukan penggantian password setelah masa kuasa penggunaan password kepada pihak lain berakhir.
(9) DPTSI harus membuat prosedur pengamanan log-on pada sistem operasi dan Database
(10) Pengamanan log-on pada sistem operasi harus diberikan kepada pengguna dalam bentuk user-id yang unik dan digunakan secara personal serta menggunakan password yang kuat sebagai teknik otentifikasi yang memadai dan terkelola secara interaktif.
(11) Ketentuan lebih lanjut tentang hak akses diatur dalam pedoman instruksi kerja tata kelola hak akses, dan instruksi kerja manajemen password untuk Administrator.

9. Manajemen Kriptografi

(1) Semua sistem yang dikelola dan/atau dikembangkan oleh DPTSI, harus menerapkan enkripsi pada hak akses (user dan password) yang dikelola.
(2) Proses enkripsi dapat dilakukan pada sistem database atau level aplikasi.
(3) Teknologi enkripsi yang digunakan harus mengikuti perkembangan teknologi kriptografi.

10. Pengamanan Akses Fisik dan Lingkungan

(1) DPTSI harus melakukan klasifikasi area kerja di institut dengan membuat table klasifikasi area kerja yaitu : VIP/terlarang, Terbatas dan Umum.
(2) Area terlarang/VIP seperti data-center dan area terbatas harus memiliki pengamanan fisik ganda, seperti pintu akses bergembok atau pengaman sidik jari.
(3) Area terlarang/VIP harus menggunakan pengamanan fisik yang dapat tahan terhadap kerusakan yang diakibatkan oleh api, banjir, gempa bumi, ledakan, kerusuhan masa dan bentuk lain dari bencana yang disebabkan oleh alam atau oleh perbuatan manusia.
(4) Setiap personil yang akan masuk ke area kerja harus memiliki identitas diri dan tercatat pada satuan pengamanan.

(5) Pihak ketiga hanya diperbolehkan masuk ke area terlarang/VIP umtuk tujuan khusus perawatan dan perbaikan yang tidak mampu dilakukan sendiri oleh DPTSI dan dalam pengawasan ketat.
(6) Seluruh lingkungan kantor dan lokasi aset informasi kritis harus terpasang kamera perekam CCTV yang aktif 24 jam dan data rekaman bisa diakses selama 30 hari terakhir.
(7) Setiap aset atau perangkat perbaikan yang akan akan masuk dan keluar dari area terlarang/VIP harus diperiksa dan diverifikasi oleh petugas DPTSI
(8) Dilarang membawa perangkat komunikasi dan media perekam apapun ketika memasuki area terlarang/VIP.
(9) Setiap proses pekerjaan penggalian di lingkungan ITS harus sepengetahuan dan mendapatkan ijin dari pihak Subdirektorat Infrastruktur dan keamanan informasi DPTSI, untuk memastikan keamanan jaringan FO yang ada di ITS.
(10) Peta jaringan FO yang ada di ITS harus terdokumentasi dan disosialisasikan ke unit-unit terkait di internal ITS.

11. Manajemen Penggunaan Sumber Daya TIK

(1) Setiap perangkat aset informasi yang digunakan harus ditempatkan pada lokasi yang aman, dan terlindung dari gangguan luar namun mudah untuk di akses.
(2) Setiap perangkat aset informasi harus mendapatkan jamiman kecukupan suplai sumber daya listrik ketika aliran listrik dari PLN padam.
(3) Setiap pemasangan kabel jaringan baik jaringan Fiber Optic ataupun jaringan LAN harus mendapatkan jaminan keamanan dari gangguan yang dapat menyebabkan kerusakan fisik atau hilangnya informasi yang ditrsnmisikan.
(4) Semua perangkat keras aset informasi harus dilakukan perawatan secara berkala sesuai dengan prosedure perawatan aset yang telah ditetapkan.

12. Manajemen Komunikasi dan Operasional

(1) Setiap seksi di DPTSI harus memiliki pedoman prosedur dan instruksi kerja untuk setiap pekerjaan.
(2) Setiap ada perubahan atau penambahan infrastruktur jaringan atau konfigurasi jaringan seksi network harus melakukan uji coba terlebih dahulu, dan ujicoba harus sepengetahuan Direktur dan Kepala Subdirektorat Infrastruktur dan Keamanan Teknologi Informasi.
(3) Subdirektorat Infrastruktur dan Keamanan Teknologi Informasi harus memiliki capacity manajement plan tentang storage, infrastruktur, dan bandwidth.
(4) Setiap ada perubahan atau penambahan pada database dan aplikasi yang dikelola oleh DPTSI harus melakukan ujicoba terlebih dahulu, dan ujicoba

harus sepengetahuan Direktur dan Kepala Subdirektorat Pengembangan Sistem Informasi.

(5) Setiap ujicoba yang dilakukan harus direncanakan dan didokumentasikan.
(6) Untuk melakukan proteksi terhadap malware dan virus pada personal computer dilingkungan ITS, DPTSI mewajibkan untuk mengunakan penggunaan sistem operasi dan aplikasi berlisensi yang terupdate. Serta melarang menggunakan perangkat lunak ilegal dalam bentuk apapun.
(7) Untuk melakukan proteksi terhadap malware pada server , DPTSI menggunakan firewall dengan proteksi terkini.
(8) Untuk back up dan recovery diatur sesuai dengan prosedur Backup dan recovery
(9) Untuk melindungi sumber daya informasi dari bencana, baik yang disebabkan oleh alam atau oleh manusia, seksi infrastruktur dan keamanan informasi harus melakukan back-up dengan membuat Disaster Recovery Center (DRC).
(10) Untuk pengelolaan dan monitoring log pada network dan network services merupakan tanggungjawab seksi infrastruktur dan keamanan informasi, sedangkan log database dan aplikasi merupakan tanggungjawab seksi pengembangan SI.
(11) Untuk manajemen log dikelola dengan software yang telah ditentukan oleh seksi infrastruktur.
(12) Log yang tersimpan hanya boleh diakses oleh administrator sistem
(13) Hasil pencatatan (file log) harus di back-up, dianalisa dan dilakukan tindakan lanjutan yang sesuai.
(14) Seksi infrastruktur dan keamanan informasi harus melakukan pengelolaan dan pengendalian jaringan dengan melakukan identifikasi setiap informasi dan sumber daya informasi yang terhubung jaringan kampus, baik jaringan yang dikelola sendiri ataupun pihak ketiga.

13. Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi

(1) Setiap pembuatan aplikasi, baik itu baru atau penambahan modul maka harus ada tahap testing
(2) Proses berbagi (sharing) data, seperti data pengajian pegawai dan dosen dan data mahasiswa pembayaran biaya pendidikan mahasiswa dengan pihak bank, dilakukan atas dasar kerjasama dan dilengkapi dengan dokumen kerjasama dan keamanan yang sangat baik dan terukur.
(3) Setiap pengembangan dan pemeliharaan sistem harus tetap memenuhi aspek kerahasiaan, keutuhan, ketersediaan, dan otentikasi serta otorisasi pada sistem informasi.

14. Hubungan dengan Supplier

(1) Proses Pengadaan barang dan jasa di DPTSI mengacu pada peraturan perundang-undangan yang berlaku.
(2) Proses pemilihan supplier untuk pengadaan barang dan jasa di DPTSI mengacu pada peraturan perundang-undangan yang berlaku.

(3) Subdirektorat Infrastruktur dan Keamanan Teknologi Informasi melakukan analisis penilaian resiko supplier barang dan jasa di DPTSI ITS.
(4) Pengelolaan perubahan jasa supplier diatur sesuai dengan peraturan perundang undangan yang berlaku.

15. Manajemen Insiden Keamanan Informasi

(1) Unit kerja DPTSI harus membuat prosedur mekanisme pelaporan dan penanganan terhadap kejadian keamanan informasi.
(2) Unit kerja DPTSI harus melakukan dokumentasi terhadap seluruh pelaporan kejadian keamanan informasi, baik yang disampaikan secara lisan maupun tertulis, baik dalam bentuk dokumen ataupun dalam bentuk elektronik (email, form elektronik dan sebagainya).
(3) Kegiatan sosialisasi, awareness dan pelatihan harus dilaksanakan kepada seluruh stakeholder ITS terhadap sistem informasi dan layanan untuk berperan serta memberikan laporan terhadap hasil pengamatan atau kecurigaan terhadap kelemahan keamanan pada sistem dan layanan di ITS.
(4) Unit kerja DPTSI harus melakukan dokumentasi terhadap seluruh kegiatan penanganan kecelakaan keamanan informasi, berdasarkan hasil tindakan perbaikan pelaksanaan, baik dari pihak internal maupun eksternal.

16. Manajemen Kontinyuitas Bisnis

(1) DPTSI harus membuat Disaster Recovery Plan (DRP) sebagai pemenuhan Business Continuity Management (BCM) aspek keamanan informasi.
(2) DPTSI harus membuat Disaster Recovery Center (DRC) sebagai tindak lanjut dokumen Disaster Recovery Plan (DRP).

17. Kepatuhan Terhadap Ketentuan yang Berlaku

(1) DPTSI melakukan pemeriksaan terhadap pemenuhan teknis standar keamanan pada sistem informasi secara berkala. Pemeriksaan pemenuhan teknis standar keamanan harus terdokumentasi, terpelihara dan dilakukan tinjauan ulang secara berkala untuk memastikan tetap *up to date* dengan kebutuhan bisnis dan perkembangan teknologi serta efektif terhadap penerapan dan pelaksanaan pemenuhan standar yang ada di ITS.
(2) DPTSI harus melakukan audit atas keefektifan penerapan dan pelaksanaan keamanan informasi dan ketidaksesuaian terhadap kebijakan keamanan, standar keamanan dan pemenuhan teknis serta hukum, undang-undang, regulasi atau kewajiban kontrak terkait keamanan informasi yang berlaku di ITS.

(3) DPTSI melakukan dokumentasi terhadap kegiatan dan hasil audit yang dilakukan untuk dilakukan tinjauan ulang oleh Rektor sebagai tindak lanjut perbaikan terhadap ketidaksesuaian di ITS.
(4) Semua pihak yang bermaksud untuk melakukan tindakan pengrusakan, mencurian dan atau penyalahgunaan informasi yang ada di lingkungan ITS ada dikenakan sanksi senagaimana undanng-undang yang berlaku