ANALISIS TINGKAT KEAMANAN APLIKASI SIMAK MENGGUNAKAN STANDARD ISO/IEC 27002:2013 BERDASARKAN CMMI
(Studi kasus : UPTTIK Universitas Siliwangi)

TESIS

Disusun sebagai salah satu syarat untuk memperoleh gelar Magister Komputer
Di Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI

Oleh:

IYOS ROSIDIN PAJAR

NPM: 2019210006

MAGISTER REKAYASA SISTEM INFORMASI

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER LIKMI

BANDUNG

2021

ANALISIS TINGKAT KEAMANAN APLIKASI SIMAK MENGGUNAKAN STANDARD ISO/IEC 27002:2013 BERDASARKAN CMMI
(Studi kasus : UPTTIK Universitas Siliwangi)

Oleh:

IYOS ROSIDIN PAJAR

NPM : 2019210006

Bandung, April 2021

Mengetahui,

Dr. Djajasukma Tjahjadi, S.E., M.T.

Pembimbing

PROGRAM STUDI PASCASARJANA MAGISTER SISTEM INFORMASI
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER LIKMI
BANDUNG
2021

HALAMAN PERSEMBAHAN

Tesis ini penulis persembahkan untuk :

1. Mamah, terimakasih mah, terimakasih untuk setiap untaian do'a mamah, dukungan mamah, juga untuk almarhum apa yang pada tanggal 8 April 2021 atau pada saat penulis melakukan sidang tesis genap 77 hari apa wafat, *hatur nuhun apa, hatur nuhun kana doa sareng dukunganna,* yang juga karena dukungan dan do'anya, penulis bisa menyelesaikan pendidikan magister di STMIK LIKMI Bandung.
2. Istri terbaik (Neng Sani Setiyani) yang selalu memberikan semangat, do'a dan tak lupa segelas kopi, terimaksih Umi, juga untuk anak tercinta (Muhhammad Abidzar Arfan Alhusayn) yang selalu menjadi obat lelah, juga untuk Mamah mertua yang selalu memeberikan dukungan dan do'a.
3. Semua pihak yang selalu mendukung dan mendo'akan.

-Hatur nuhun-

ABSTRAK

ANALISIS TINGKAT KEAMANAN APLIKASI SIMAK MENGGUNAKAN STANDARD ISO/IEC 27002:2013 BERDASARKAN CMMI (Studi kasus : UPTTIK Universitas Siliwangi)

Oleh :

IYOS ROSIDIN PAJAR
NPM.2019210006

Salah satu permasalahan yang dibawa serta dalam perkembangan teknologi informasi adalah permasalahan keamanan, keamanan data menjadi suatu hal yang menarik untuk di cermati. Universitas Siliwangi adalah salah satu bidang pendidikan yang memanfaatkan teknologi informasi dalam menjalankan proses bisnisnya, salah satu teknologi informasi yang digunakannya adalah aplikasi SIMAK, Penelitian yang dilakukan yaitu untuk mengetahui tingkat keamanan dari aplikasi SIMAK.

Untuk selanjutnya peneliti dapat memberikan sebuah rekomendasi kepada pengelola SIMAK yang akan menjadi dasar perbaikan yang harus dilakukan dimasa yang akan datang terkait keamanan data. Dalam penelitian ini, peneliti menggunakan 4 domain dari ISO/IEC 27002:2013 yaitu domain 5 berisi kebijakan keamanan informasi, domain 6 berisi keamanan informasi organisasi, domain 9 berisi kontrol akses dan domain 11 berisi dengan keamanan fisik dan lingkungan, jika dirinci dari keempat domain tersebut didapat 38 kontrol keamanan.

Dari hasil kuesioner dan pembobotan maka dihitung tingkat kematangan pada setiap domain yang di teliti, maka didapatkan hasil kematangan sebagai berikut : domain 5 nilai kematangan = 1,49, domain 6 nilai kematangan = 1,52, domain 9 nilai kematangan = 1,32 dan domain 11 nilai kematangan = 1,97 dan apabila di rata – ratakan bahwa aplikasi SIMAK Universitas Siliwangi kini berada pada *level* 2 atau *repeatable.*

Kata Kunci: Aplikasi SIMAK, Sistem Informasi Akademik, Keamanan Sistem Informasi, Tingkat Kematangan, ISO 27002, CMMI.

ABSTRACT

ANALYSIS OF APPLICATION SECURITY LEVELS USING ISO / IEC 27002: 2013 STANDARD BASED ON CMMI (Case study: UPTTIK Siliwangi University)

By:
IYOS ROSIDIN PAJAR
NPM.201921006

One of the problems brought about in the development of information technology is the problem of security, data security is an interesting thing to observe. Siliwangi University is one of the fields of education that utilizes information technology in carrying out its business processes, one of the information technologies it uses is the SIMAK application. Research conducted is to determine the level of security of the SIMAK application.

Henceforth, the researcher can provide a recommendation to the SIMAK manager which will be the basis for improvements that must be made in the future regarding data security. In this study, researchers used 4 domains from ISO / IEC 27002: 2013, namely domain 5 contains information security policies, domain 6 contains organizational information security, domain 9 contains access control and domain 11 contains physical and environmental security, if specified from the four domains. obtained 38 security controls.

From the results of the questionnaire and weighting, the maturity level of each domain under study is calculated, so the results of maturity are as follows: domain 5 maturity value = 1.49, domain 6 maturity value = 1.52, domain 9 maturity value = 1.32 and domain 11 maturity value = 1.97 and if on average, the SIMAK application at Siliwangi University is now at level 2 or repeatable.

Keywords: *SIMAK Application, Academic Information System, System Information Security, Maturity Level, IS0 27002, CMMI*

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke khadirat Alloh SWT, yang dengan qodo dan qadar-Nya telah memberikan kelancaran kepada penulis sehingga dapat menyelesaikan penelitian yang diberi judul "**ANALISIS TINGKAT KEAMANAN APLIKASI SIMAK MENGGUNAKAN STANDARD ISO/IEC 27002:2013 BERDASARKAN CMMI (Studi kasus : UPTTIK Universitas Siliwangi)".**

Tesis ini disusun guna memperoleh gelar Magister pada program studi Pascasarjana Magister Sistem Informasi.

Penulis mengucapkan terimakasih yang tak terhingga atas bimbingan dan dukungannya kepada :

1. Dr. Djajasukma Tjahjadi, S.E., M.T. selaku pembimbing dalam penyusunan tesis ini, yang sudah membantu dalam penyelesaian penelitian ini.
2. Pimpinan dan seluruh staff UPTTIK Universitas Siliwangi yang telah memperkenankan penulis untuk melakukan penelitian ditempat tersebut.
3. Kedua orang tua, (Apa, Mamah) yang tanpa henti memberikan dukungan moril maupun materil juga dukungan do'a.
4. Istri terbaik (Neng Sani Setiyani) dan anak terhebat (Muhammad Abidzar Arfan Alhusayn) yang telah memberikan semangat dan do'a terbaik, juga untuk mamah Ciawi yang selalu memeberikan dukungan dan do'a.
5. Rekan – rekan angkatan 2019, yang telah membatu dan memberikan semangat dalam menyelesaikan penyusunan tesis ini.
6. Juga semua pihak yang tidak dapat disebutkan satu persatu.

Bandung, April 2021

Penulis

DAFTRAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan dan kebutuhan akan sistem informasi saat ini menarik untuk diamati. Hampir semua bidang kini memerlukan bahkan ketergantungan akan sistem informasi. Dalam proses perancangannya, kebutuhan akan sistem informasi dilakukan dengan menganalisa dan memperhatikan dua aspek yaitu kebutuhan fungsional dan kebutuhan non fungsional. Kebutuhan fungsional adalah kebutuhan yang didalamnya berisi proses – proses yang nantinya dilakukan oleh sistem. Sedangkan kebutuhan non fungsional adalah kebutuhan yang menitik beratkan pada properti prilaku yang dimiliki oleh sistem. Perguruan tinggi di Indonesia sebagai salah satu bidang yang memanfaatkan teknologi informasi. Diilhami dari perkembangan teknologi informasi proses bisnis telah bergeser dari proses bisnis yang menggunakan cara tradisional ke cara yang lebih efisien serta meningkatkan komunikasi antara perusahaan dan pemasok (Hall, 2011).

Salah satu bidang yang memanfaatkan teknologi informasi dalam menunjang kelancaran operasionalnya adalah bidang pendidikan, selain itu bidang pendidikan memanfaatkan kemajuan teknologi informasi untuk pengolahan data dan untuk kelancaran penyampaian informasi kepada peserta didik. Selain peserta didik, pemanfaatan teknologi informasi juga dimaksudkan untuk dapat membantu tenaga pengajar dan tenaga administrasi dalam menyelesaikan tugas yang berhubungan dengan akademik. Sejalan dengan hal tersebut, semakin banyak pengguna yang memanfaatkan teknologi informasi dalam melakukan aktifitasnya persoalan baru muncul, persoalan tersebut adalah persoalan keamanan yaitu mudahnya sistem disusupi oleh pihak yang tidak bertanggungjawab dan dapat mengancam keutuhan data yang tersimpan pada sistem informasi tersebut.

Rahardjo (2005) mengungkapkan bahwa keamanan adalah merupakan salah satu aspek penting pada sebuah sistem informasi. Dengan kata lain sebuah sistem informasi haruslah dapat menjaga keamanannya, keamanan yang dimaksud mencakup keamanan internal dan eksternal organisasi. Masalah yang terjadi pada aplikasi atau sistem informasi

berpotensi menimbulkan kerugian bagi organisasi, mengingat data yang diolah oleh sebuah aplikasi merupakan data penting dari perusahaan atau organisasi. Masalah yang terjadi dapat berupa berhenti bekerjanya aplikasi, kesalahan penginputan data akibat *human error,* sampai dengan kehilangan data. Ketika penerapan teknologi informasi pada bidang pendidikan dilakukan, permasalahan yang kerap muncul adalah permasalahan keamanan data, permasalahan yang menyangkut data menjadi hal yang sering terjadi, misalnya rusaknya data, bahkan sampai hilangnya data, permsalahan tersebut muncul bisa karena faktor kecerobohan pengguna atau dikarenakan gangguan dari pihak eksternal, yang lebih berbahaya adalah ketika pengguna tidak menyadari bahwa data yang dikelolanya adalah data yang bersifat rahasia dan harus diamankan. Selanjutnya, permasalahan yang kerap terjadi adalah terkait dengan hak akses pengguna, dimana pengguna dapat mengakses suatu data atau sistem yang bukan menjadi hak aksesnya yang tentu saja dapat mengancam kerahasiaan suatu data. Kebocoran data rahasia tentu saja dapat memicu atau bahkan menimbulkan kerugian pada organisasi. (Hermaduanti, 2016) mengungkapkan salah satu aspek yang penting dari sebuah sistem informasi adalah masalah keamanan, dimana bisa saja orang yang tidak bertanggung jawab dapat masuk kedalam sistem melalui jaringan yang tersedia.

UPTTIK Universitas Siliwangi adalah salah satu organisasi yang memanfaatkan teknologi informasi dalam menopang kelancaran proses akademik, namun selama ini UPTTIK sebagai pengelola sistem belum menganalisa dan menerapkan standar yang dapat menjamin keamanan data yang ada pada sistem informasinya. Setelah melakukan analisa dari permasalahan diatas, UPTTIK sebagai pengelola sistem di Universitas Siliwangi harus melakukan evaluasi terhadap aspek – aspek yang berhubungan dengan permasalahan sistem informasi yang dikelolanya supaya dapat meminimalisir munculnya gangguan dan menjamin keamanan data pada sistem informasinya. Hal ini dilakukan untuk menjaga kerahasiaan, keutuhan dan ketersediaan *(Confidentality, Integrity, Avalability)* (ISO/IEC 27002, 2005:1).

Diperlukan pengukuran kinerja melalui pemeriksaan, supaya sitem berjalan sebagaimana mestinya, juga dipelukan penerapan standar baku supaya pemeriksaan berjalan dengan baik (Rosmiati, 2016).

Diperlukan suatu standar untuk melakukan audit pada sistem informasi untuk menjamin sistem informasi berjalan dengan baik dan dapat menjamin keamanan data (Tanuwijaya & Sarno, 2010).

Dalam melaksanaan pemeriksaan sistem informasi, tidak ada acuan baku bagi perusahaan atau organisasi untuk melaksanakan pemeriksaan (Syafrizal, 2007). Pemilihan dan penentuan standar oleh UPTTIK sebagai pengelola sistem informasi yang berada di Universitas Siliwangi menggunakan standar yang dikeluarkan oleh ISO/IEC 27002:2013.

Alasan pemilihan ISO/IEC 27002:2013 dipilih oleh UPTTIK menjadi standar keamanan pada sistem informasi yang dikelolanya adalah karena ISO/IEC 27002:2013 bersifat fleksibel, mudah dikembangan menyesuaikan dengan kebutuhan organisasi, kebutuhan organisasi, persyaratan keamanan, sampai ukuran organisasi yang memakainya.

Terkait dengan model perhitungan yang akan digunakan sebagai acuan perhitungan tingakat kematangan dan keamanan adalah menggunakan CMMI. CMMI adalah kepanjangan dari *Capability Maturity Model Integration.*

Dengan dilakukannya audit atau pemeriksaan keamanan pada aplikasi SIMAK yang dikelola oleh UPTTIK Universitas Siliwangi maka akan dapat diketahui kelemahan – kelemahan yang terdapat pada aplikasi tersebut yang menjadi penyebab munculnya permasalahan keamanan informasi yang selama ini kerap terjadi. Selain itu, pemeriksaan ini dapat mengukur tingkat keamanan sistem informasi yang dimiliki oleh Sistem Informasi Akademik (SIMAK) Universitas Siliwangi. Setelah selesai melakukan pemeriksaan maka penulis dapat merekomendasikan tentang langkah perbaikan yang harus dilakukan untuk meningkatkan keamanan informasi pada aplikasi SIMAK, selain itu langkah itu juga dapat menjadi pertimbangan dan acuan apabila pengelola sistem akan mengajukan ISMS *certification* dengan standar ISO 27002 di masa mendatang.

1.2 Rumusan Masalah

Berdasarkan penjelasan pada latar belakang, maka didapat rumusan malsah sebagai berikut :

1. Apakah aplikasi SIMAK yang dikelola oleh UPTTIK Universitas Siliwangi sudah sesuai dengan standar ISO 27002, dan sejauh mana kesiapan aplikasi SIMAK dalam penerapan standar ISO 27002?
2. Apa dan bagaimana peranan standarisasi keamanan sistem informasi dalam menjaga keamanan informasi yang tersimpan dari berbagai ancaman yang kerap muncul?
3. Bagaimana cara menyusun hasil pemeriksaan keamanan aplikasi SIMAK berdasarkan standar ISO 27002?

1.3 Batasan Masalah

Berdasarkan penjelasan pada latar belakang diatas, maka disepakati Batasan masalah adalah sebagai berikut :

1. Domain ISO 27002 : 2013 yang digunakan sesuai yaitu hasil dari diskusi dengan dengan pimpinan UPTTIK Universitas Siliwangi sebagai pengelola dari aplikasi SIMAK, selain daripada itu, penentuan domain atau klausul juga didasari dari kebutuhan organisasi itu sendiri yaitu:
   a. Domain A.5 : domain berisi terkait kebijakan keamanan informasi.
   b. Domain A.6 : domain berisi terkait keamanan informasi organisasi.
   c. Domain A.9 : domain berisi terkait kontrol akses.
   d. Domain A.11 : domain berisi terkait Keamanan fisik dan lingkungan.
2. Ruang lingkup pemeriksaan sistem informasi hanya mencakup pada sistem informasi atau aplikasi SIMAK yang dikelola oleh UPTTIK Universitas Siliwangi.

1.4 Tujuan Penelitian

Sitem informasi kemahasiswaan banyak digunakan oleh perguruan tinggi dalam mengelola data terkait akademik dan kemahasiswaan, salah satu yang penggunakan

sistem informasi akademik adalah Universitas Siliwangi yang dalam hal ini menjadi tanggungjawab UPTTIK Universitas Siliwangi. Pengelolaan terkait sistem informasi akademik atau aplikasi SIMAK di Universitas Siliwangi saat ini belum merujuk kepada suatu standar baku, termasuk pengelolaan infrastruktur penunjang aplikasi SIMAK belum dikelola secara optimal. Selain daripada itu, isu keamanan *cyber* terkait aplikasi dan keamanan data pada aplikasi SIMAK juga belum mendapatkan perhatian serius dari pihak terkait ataupun pemangku kebijakan di Universitas Siliwangi.

Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN) kejahatan atau serangan *cyber* tercatat terjadi 88.414.296 kasus yag terjadi sejak 1 Januari hingga 12 April 2020, hal ini tentu saja harus mendaatkan perhatian yang serius dari UPTTIK sebagai penanggungjawab atau pengelola aplikasi SIMAK, langkah – langkah pencegahan terkait keamanan *cyber* mutalak perlu dilakuakan dan dipersiapkan supaya kerugian yang diakibatkan oleh kejahatan *cyber* dapat dihindari, langkah preventif perlu diambil untuk mempersiapkan dari hal terburuk yang mungkin terjadi terhadap keamanan aplikasi SIMAK dan infrastruktur pendukung.

Selain dari pada isu keamanan *cyber,* keamanan secara fisik juga belum mendapatkan perhatian secara serius, menurut pengamatan yang dilakukan oleh penulis di lokasi penelitain yaitu di ruangan UPTTIK Universiatas Siliwangi, infrastruktur ruangan sever aplikasi SIMAK yang juga tempat dimana *server* aplikasi lain berada belum merujuk kepada standar ruangan *server* yang sesuai, pengelolaan *server* pada UPTTIK Universitas Siliwangi belum mengacu kepada ketentuan manajemen server yang disesuaikan dengan standar pengelolaan data *server* seperti menurut *Telecommunications Industry Association (TIA)* 942.

UPTTIK sendiri selain bertanggungjawab atas aplikasi SIMAK, juga mengelola lebih dari 15 *server* dan lebih dari 15 aplikasi, seluruh aplikkasi dan *server* tersebut belum satu pun yang sudah dilakukan audit terkait keamanan, baik keamanan aplikasi ataupun keamanan infrastrukktur pendukungnya. Hal tersebut juga yang mendasari perlunya dilakukan suatu audit terhadap aplikasi SIMAK sebagai *pilot project* untuk audit aplikasi dan infrastruktur lainnya dikemudian hari.

Secara singkat penelitian ini didasarkan atas kebutuhan organisasi yaitu UPTTIK Universitas Siliwangi sebagai pengelola sistem informasi dalam rangka untuk mempunyai sistem informasi yang berjalan sebagai mana mestinya juga sesuai dengan standar keamanan, selain itu juga penelitian ini dilakukan untuk mengetahui adanya kemungkinan ketidak sesuaian atau penyimpangan pada sistem yang sedang berjalan, selanjutnya setelah diselesaikannya penelitian ini dihasilkan umpan balik yang dapat ditindak lanjuti oleh organisasi dalam mengelola sistem informasi dan dilakukan penyesuaian dan perbaikan oleh pihak terkait dimasa mendatang, selain daripada itu penelitian ini adalah langkah awal organisasi untuk mempersiapkan dalam menghadapi sertifikasi ISO 27002.

Setelah menganalisa dan merumuskan masalah yang sebelumnya telah dijelaskan, maka ada beberapa tujuan yang ingin dicapai setelah penelitian ini selesai dilakukan. Tujuan yang ingin dicapai adalah :

1. Diharapakan dari hasil penelitian ini menghasilkan sebuah pengukuran yang tepat terkait dengan keamanan informasi pada aplikasi SIMAK yang dikelola oleh UPTTIK Universitas Siliwangi, serta selanjutnya dapat menghasilkan sistem informasi yang menjamin keamanan data sesuai dengan standar yang telah ditentukan yaitu ISO/IEC 27002:2013.
2. Penelitan dapat mengetahui tentang tingkat kematangan dari aplikasi SIMAK menggunakan perhitungan yang telah ditentukan yaitu menggunakan CMMI.
3. Hasil dari analisa penelitian mengenai aplikasi simak yang dikelola oleh UPTTIK Universitas Siliwangi berdasarkan ISO/IEC 27002:2013 dan CMMI ini selanjutnya disusun kedalam sebuah laporan. Laporan berisi temuan – temuan dan rekomendasi yang harus dilakukan dan dapat di implementasikan dimasa mendatang oleh pihak UPTTIK Universitas Siliwangi.

1.5 Manfaat Penelitian

Manfaat dari penelitian bagi penulis dan bagi UPTTIK Universitas adalah :

1. Terciptanya sistem akademik yang aman dan sesuai standar ISO/IEC 27002:2013 yang dikelola oleh UPTTIK.

2. Bagi UPTTIK atau lembaga (Universitas Siliwangi) tidak perlu mengeluarkan anggaran untuk melakukan audit keamanan informasi terhadap aplikasi SIMAK namun bisa melakukan perbaikan dan penyesuaian terhadap keamanan sistem secara mandiri.
3. Manfaat tidak hanya bagi UPTTIK sebagai pengelola sistem, manfaat juga dapat dirasakan oleh penulis dengan bertambahnya pengetahuan dan pemahaman tentang standar keamanan informasi.
4. Selanjutnya, bagi pengguna utama dari aplikasi SIMAK yaitu mahasiswa adalah terlindunginya data yang tersimpan pada aplikasi SIMAK, mengingat data yang tersimpan adalah termasuk data rahasia yaitu data pribadi mahasiswa itu sendiri.

1.6 Jenis Penelitian

Metode yang dipakai penulis dalam peneletian ini adalah menggunakan metode kuantitatif, dimana data yang diperoleh dan diolah penulis adalah hasil dari penyebaran kuisioner kepada responden, responden dalam penelitian ini adalah seluruh anggota UPTTIK Universitas Siliwangi yang berjumlah 7 orang.

Purposive sampling adalah teknik pengambilan *sample* yang dilakukan oleh penulis, pada penelitian ini *sample* dipilih berdasarkan pada tugas poko dan keahlian masing – masing responden.

1.7 Sistematika Penulisan dan Pengumpulan Data

Sistematika penulisan dapat membantu memahami alur berfikir keseluruhan pada tesis ini adalah sebagai berikut :

Bab I Pendahuluan

Bab ini terdiri dari latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, serta sistematika penulisan.

Bab II

Bab ini mencakup landasan teori, kerangka berfikir, dan penelitian terdahulu terkait ISO 27000 series dan *Maturity Model.*

Bab III

Bab ini pencakup objek, waktu dan lokasi penelitian, sumber data dan penerapan ISO/IEC 27002:2013 dan CMMI.

Bab IV

Pada bab ini terdapat hasil penelitian dan pembahasan mengenai penelitian yang telah dilakukan tentang ISO/IEC 27002:2013 dan CMMI.

Bab V Penutup

Pada bab ini selain kesimpualan juga terdapat saran.

Pada penelitian ini data yang didapat dibagi menjadi dua jenis data, yaitu data utama dan data pendukung. Data utama diperoleh melalui :

1. Observasi adalah langkah pertama yang dilakukan penulis dalam pengumpulan data, yaitu dengan cara pengamatan secara langsung, melihat penerapan aplikasi SIMAK, cara kerja UPTTIK khusunya yang menyangkut dengan poin domain atau klausul yang akan penulis teliti.
2. Wawancara, data diperoleh dengan cara mengajukan pertanyaan kepada narasumber merangkap sebagai responden, responden ini adalah pegawai dari UPTTIK selaku pemegang dan penanggungjawab aplikasi SIMAK yang berasal dari lingkungan Universitas Siliwangi.
3. Survei, data yang diperoleh dari survei yaitu dengan mengajukan kuisioner kepada responden, pemilihan responden adalah sebagai sampling. Selain itu juga dilakukan pengamatan secara langsung terkait bukti – bukti yang ada dilapangan.

1.8 Penentuan Responden

Responden pada penelitian ini adalah 7 orang pegawai atau karyawan UPTTIK Universiatas Siliwangi, hal ini dilakukan mengingat penelitian ini bertempat di UPTTIK, juga penelitian yang dilakukan adalah seputar pengelolaan aplikasi SIMAK, oleh karena hal tersebut ketujuh pegawai UPTTIK adalah orang yang dianggap paling mengetahui dan bertanggungjawab terhadap pengelolaan aplikasi SIMAK.

Kontrol dibuat untuk memastikan bahwa tindakan organisasi sudah sesuai prosedur dan tujuan organisasi, selain itu juga untuk memastikan kejadian yang tidak diinginkan dapat dicegah atau bisa diperbaiki secara dini. Tabel 1.1 adalah pemetaan yang telah disepakati untuk dilakukan penelitian yang merujuk pada standar ISO 27002.

Tabel 1. 1 Tabel domain cakupan penelitian

Domain	Keterangan
A.5	domain berisi terkait kebijakan keamanan informasi.
A.6	domain berisi terkait keamanan informasi organisasi
A.9	domain berisi terkait kontrol akses.
A.11	domain berisi terkait Keamanan fisik dan lingkungan.

Sumber : ISO 27002:2013

Kuisioner yang dibuat oleh penulis dan diserahkan kepada responden merupanakan kuisioner yang berisikan pertanyaan yang berdasarkan pada ISO 27002:2013 yang berisikan tentang manajemen keamanan informasi.

BAB II

LANDASAN TEORI

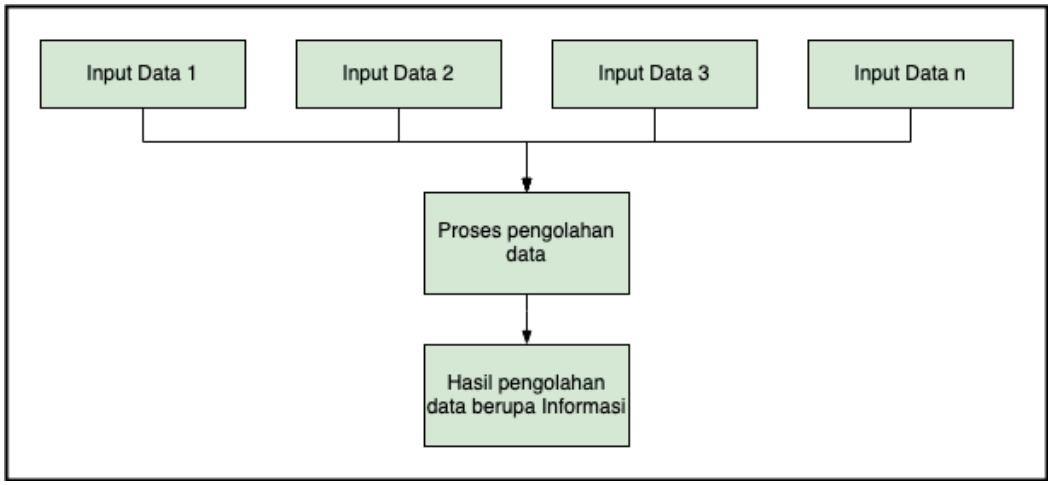
2.1 Sistem Informasi

Sistem informasi adalah kombinasi dari manusia, perangkat keras, perangkat lunak, jaringan dan sumberdaya lainnya yang mengumpulkan, mengolah dan mengubah data dan menyebarkannya pada suatu organisasi (Yakub, 2012).

(Marakas dan O'Brien, 2017) mengungkapkan sistem informasi adalah gabungan teratur dari perangkat keras, perangkat lunak, jaringan, data dan kebijakan serta prosedur mengumpulkan, menghimpun, mengolah data menyebarkan data sampai mendapatan data kembali pada suatu organisasi.

(Riadi, Imam, 2013) mengungkapkan bahawa dalam pembangunan aplikasi yang mendukung jaringan *forensic* adalah persoalan bagaimana menentukan metode yang tepat untuk memudahkan pengolahan data log menjadi data yang mudah diproses. Keberhasilan suatu sistem informasi yang diukur berdasarkan tujuan pembuatannya bergantung pada tiga faktor utama, yaitu keselarasan dan kualitas data, pengorganisasian data, dan proses penggunaan informasi untuk memenuhi kebutuhan penggunaan tertentu.

Sistem informasi mengumpulkan data dari berbagai sumber yang kemudian dihimpun. Data yang terhimpun kemudian digambungkan menjadi satu kesatuan dan menghasilkan sebuah informasi. Sistem informasi yang baik haruslah mempunyai sifat ketergabungan data satu dengan data yang lain.



Gambar 2. 1 Proses umum sistem informasi

Sumber : Imam Riadi (2013)

Beberapa ahli mengungkapkan pengertian sistem informasi, diantaranya adalah sebagai berikut :

1. Sistem informasi adalah gabungan yang teratur dari *hardware, software, network,* kebijakan, dan data bertugas untuk mengumpulkan dan menghimpun selanjutnya mengolah dan mendistribusikan data sampai akhirnya mendapatkan data kembali (O'Brien, A. James. G. M. Marakas, 2016).
2. Dalam membangun sebuah aplikasi yang mempunyai dukungan *forensic network* adalah tentang penentuan metode yang cocok untuk mempermudah dalam proses pengolahan data *log* menjadi suatu data yang mudah untuk diproses (Riadi, Imam, J. E. Istiyanto, A. Ashari, Subanar, 2013).
3. Sistem Informasi merupakan sekumpulan elemen atau subsistem yang digabungkan, saling keterkaitan atau berhubungan bertugas untuk mengelola dan mengolah data sehingga menjadi berarti bagi penerima, selain itu juga berfungsi untuk penentuan keputusan dimasa mendatang. (Nugroho, Anggun, 2015).
4. Sitem informasi merupakan sebuah sistem yang terdapat pada suatu organisasi yang berfungsi untuk mendukung organisasi pada bidang manajerial, dapat bekerja melakukan transaksi harian, dan menghasilkan laporan untuk kebutuhan pihak eksternal (Jeperson Hutahaean, 2014).

5. Sistem informasi merupakan suatu perkumpulan data yang terorganisasi dilengkapi dengan tata cara atau prosedur penggunaan mencakup lebih jauh dari sebuah perjanjian, istilah tersebut menyiratkan suatu maksud yang ingin dicapai dengan jalan memilih dan mengatur data serta menyusun tatacara penggunaanya (Krismaji, 2015).

Disimpulkan pengertian dari sistem informasi adalah kumpulan sumberdaya yang berupa alat atau manusia serta modal yang terintegrasi, bekerja menghimpun dan mengolah data serta menghasilkan informasi pada semua tingkatan operasional yang dapat digunakan untuk perencanaan, pelaksanaan, pekerjaan, pengendaliann serta pengambilan keputusan.

Tujuh ciri sistem informasi yang berkualitas meneurut Raymod Mc. Leod (2008) adalah sebagai berikut :

1. Akurat, informasi yang baik harus mencerminkan kondisi yang sebenarnya. Hal ini bisa dibuktikan dengan adanya pengujian oleh dua orang atau lebih dan ketika menghasilkan hasil yang sama maka informasi tersebut bisa dianggap akurat atau berkualitas.
2. Tepat waktu, data bisa dikatakan berkualitas apabila tersedia pada waktu yang diperlukan, dengan kata lain data harus selalu tersedia kapanpun di butuhkan.
3. Relevan, atau harus sesuai dengan yang diperlukan, artinya selain tersedia, data juga harus sesuai dengang apa yang diperluakan oleh organisasi.
4. Lengkap, informasi yang tersedia haruslah dalam keadaan lengkap, tan tidak terbagi bagi atau tidak ada sesuatu yang kurang.
5. *Correctless*, berarti tidak ada kesalahan, data yang tersedia dapat dikatakan berkualitas apabila tidak ada kesalahan didalamnya atau memiliki tingkat kebenaran yang baik.
6. *Security*, berarti informasi yang dihasilkan mempunyai manfaat yang lebih besar

dibandingkan dengan biaya mendapatkannya dan sebagian besar informasi tidak dapat ditaksir keuntungannya dan dengan satuan nilai uang tetapi dapat ditaksir nilai efektifitasannya.

2.2 Sistem Informasi Akademik

Menurut Andi (2010), pengertian dari sistem informasi akademik adalah suatu sistem yang mempunyai fungsi khusus yaitu pengolahan data – data akademik, penerapanya melaui kombinasi antara *hardware* dan *software*, yang dimaksud dengan *hardware* adalah komputer, *printer*, dan lain sebagainya, sedangkan yang dimaksud dengan *software* adalah program yang berfungsi menghubungkan atau menjalankan *hardware*.

Lebih spesifik, menurut Amarusu (2013), sistem informasi akademik adalah sistem yang secara khusus dibangun untuk memenuhi kebutuahan perguruan tinggi. Tujuannya adalah untuk meningkatkan layanan, kinerja SDM dan daya saing perguruan tinggi. Singkatnya sistem informasi akademik adalah sebuah aplikasi yang diciptakan untuk membantu memudahkan perguruan tinggi dalam mengolah data – data akademik.

Universitas Siliwangi adalah salah satu perguruan tinggi yang memanfaatkan sistem informasi akademik sebagai sarana penunjang kelancaran pengolahan data akademik, data akademik yang dimaksud mencakup data mahasiswa, data dosen, data matakuliah sampai data keuangan mahasiswa.

Tujuan pengolahan data akademik adalah untuk mendorong kegiatan pengajaran dengan dukungan organisasi manajemen yang bersih dan terstruktur, menampilkan informasi penting dalam bentuk tertulis, dan menyimpan semua dokumen.

Sistem yang digunakan memanfaatkan jaringan internet untuk menjalankannya, oleh karena itu informasi dapat diakses tidak hanya di dalam kampus saja, namun juga dapat diakses di luar kampus selama ada media seperti komputer atau *smartphone* yang terhubung ke jaringan internet. Sistem informasi akademik adalah merupakan sistem informasi yang berbasis web yang bertujuan untuk membentuk *Knowledge Based System*

yang dapat diakses internet, sebagai contoh macam informasi yang ada didalamnya adalah :

1. Data mahasiswa, berisi tentang data pribadi mahasiswa, mencakup nama lengkap, data keluarga, data keuangan mahasiswa, data orang tua, pekerjaan orang tua, sampai asal sekolah mahasiswa.
2. Data akademik, berisi informasi yang berkaitan dengan akademik atau perkuliahan, seperti data mata kuliah, jadwal kulah, waktu yudisium, data kerja praktek, dosen pengampu, data tugas akhir, data jadwal kuliah, materi matakuliah, sampai penelitain dan pengabdian.
3. Data perkuliahan, berisi tentang, jumlah kehadiran mahasiswa, sampai jadwal perkuliahan dosen.
4. Data keuangan, berisi informasi tentang data keuangan mahasiswa, herregistrasi mahasiswa, sampai tunggakan mahasiswa.

2.3 Keamanan Informasi

Keamanan Informasi adalah upaya untuk melakukan perlindungan terhadap berbagai macam ancaman bertujuan untuk memastikan keberlangsungan bisinis, meminimalisir risiko, juga meningkatkan peluang dan investasi bisnis pada organisasi. (ISO/IEC 17799:2005).

Keamanan informasi adalah suatu upaya untuk mengamankan aset informasi terhadap ancaman yang mungkin timbul. Sehingga keamanan informasi secara tidak langsung dapat menjamin kontinuitas bisnis, mengurangi risiko – risiko yang terjadi, mengoptimalkan pengembalian investasi *(return on investment)*. Semakin banyak informasi perusahaan yang disimpan, dikelola dan di-*sharing*-kan maka semakin besar pula risiko terjadi kerusakan, kehilangan atau terekseposnya data ke pihak eksternal yang tidak diinginkan (Sarno dan Iffano : 2009).

Beberapa contoh terkait keamanan informasi menurut Sarno dan Iffano (2009: 27) dikelompokan sebagai berikut :

1. *Physical Security* adalah strategi mengamankan dan melindungi pekerja, aset fisik, dan tempat kerja dari ancaman yang merugikan perusahaan atau organisasi seperti bencana alam, atau bencana yang sebabkan oleh orang yang tidak bertanggung jawab dan akses tanpa otoritas.
2. *Personal Security* adalah strategi yang memfokuskan pada perlindungan individu berupa pemahaman kan pentingnya keamanan informasi. Biasanya saling berhubungan dengan ruang lingkup *"physical security".*
3. *Operation Security* adalah keamanan informasi yang berisi strategi organisasi berupa kemampuan untuk mengamankan organisasi supaya dapat berjalan tanpa hambatan.
4. *Communications Security* adalah keamanan informasi yang mempunya tujuan untuk mengamankan alat komunikasi, teknologi komunikasi dan segala sesuatu yang menjadi bagian didalamnya. Serta kemampuan organisasi dalam memanfaatkan media informasi untuk dapat mencapai tujuan dari organisasi.
5. *Network Security* adalah kemampuan organisasi dalam melindungi organisasi pada sisi jaringan, dan memanfaatkan jaringan untuk memenuhi kebutuhan organisasi pada sisi komunikasi.

Keamanan informasi terdiri dari tiga aspek yang sering disingkat menjadi CIA yaitu *Convidentiality* (Kerahasiaan), *Integrity* (Keaslian) dan *Availability* (Ketersediaan). Ketiga aspek tersebut dirincikan sebagai berikut :

1. *Confidentiality* : Suatu sistem informasi haruslah menjamin kerahasiaan dari data yang terkandung didalamnya, kerahasiaan ini maksudnya adalah, data haruslah dapat diakses oleh orang berhak atas data tersebut.
2. *Integrity* : Keaslian data adalah aspek selanjutnya yang harus dimiliki oleh sistem informasi, keaslian disini maksudnya adalah data harus terlindungi dan tetap terjaga keasliannya.
3. *Availability* : atau ketersediaan adalah Keamanan Informasi harus menjamin

pengguna supaya tetap dapat mengakses data tanpa adanya gangguan. Pengguna yang dimaksud adalah manusia ataupun komputer yang mempunyai otoritas atau hak atas data tersebut.

2.4 Standar Manajemen Keamanan Sistem Informasi

Sistem informasi pada pada suatu organisasi haruslah mempunyai standar dalam menyajikan informasi kepada pengguna, hal ini dimaksudkan untuk menjamin data yang disajikan tetap aman dari akses atau gangguan pihak lain yang tidak berhak atas data tersebut, salah satu standar keamanan informasi yang sering dipakai oleh perusahaan atau organisasi – organisasi dunia adalah ISO/IEC 27000 *series*.

Sistem Manajemen Keamanan Informasi (SMKI) atau yang biasa dikenal sebagai ISMS *(Information Security Management System)* merupakan suatu standar sistem keamanan informasi yang diterbitkan oleh ISO dan IEC, berdampingan antara ISO/IEC 27001 dan 27002 memberikan daftar tujuan pengendalian dan merekomendasikan suatu rangkaian pengendalian keamanan spesifik.

Suatu perusahaan yang sudah menerapkan SMKI, kemungkinan akan mampu mengendalikan aset informasi dari adanya ancaman dan serangan, secara tidak langsung memberikan jaminan terhadap kelangsungan bisnis perusahaan.

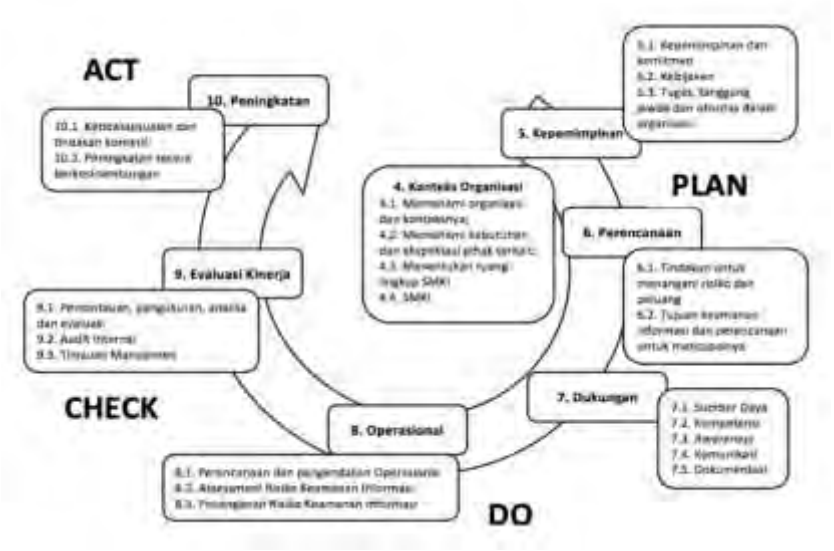
ISO merupakan organisasi luar dari pemerintahan atau biasa disebut dengan *(Non-Government Organization/NGO),* ISO beranggotakan badan – badan standarisasi yang berasal lebih dari 140 negara, ISO berdiri sejak 1947. Fungsi dari ISO adalah untuk memberikan dukungan pengembangan dari standarisasi, awalnya dimaksudkan untuk membantu dalam bidang perdagangan internasional, selain itu juga dimaksudkan dalam upaya mendukung dalam hal pendidikan dan pengembangan di bidang ilmu pengetahuan, teknologi sampai bidang ekonomi. Kegiatan pokok ISO adalah menghasilkan kesepakatan – kesepakatan internasional yang kemudian dipublikasikan sebagai standar internasional.

Dalam mengembangkan standar ini, mereka mengundang perwakilan dari 130 negara untuk berpartisipasi dalam pertemuan Komite Teknis (TC), Subkomite (SC) dan

Kelompok Kerja (WG). Peserta ISO termasuk badan standar nasional dari masing – masing negara dan perusahaan besar. ISO bekerja sama dengan *International Electrotechnical Commission* (IEC), yang bertanggung jawab atas standarisasi peralatan elektronik.

Information Security Management (ISO) mulai mengembangkan standar terkait *Information Security management System (ISMS)* atau Sistem Manaajemen Keamanan Informasi (SMKI) sejak tahun 2005, pengembangan tersebut berupa panduan juga dalam bentuk persyaratan standar.

ISO 27000 dikeluarkan pada atahun 2009, didalamnya terdapat 46 standar keamanan dasar yang didefinisikan dalam dalam *"Term and Condition"* ISO 27000. Keamanan informasi tersebut didasarkan pada perusahaan yang bisnis prosesnya tegantung pada infrastruktur IT yang rentan terhadap gangguan dan kegagalan. Standar teknologi informasi ini sama halnya dengan standar informasi yang lain yaitu mengacu kepada siklus PDCA *(PLAN – DO – CHECK – ACTION)*, siklus ini terkendal dengan manajemen mutu.



Gambar 2. 2 Siklus PDCA ISO 27001

Sumber : A.T. Kearney Analysis, 2013

Model *PLAN – DO – CHECK – ACT* (PDCA) diterapkan terhadap struktur keseluruhan proses sistem manajemen keamanan informasi (SMKI). Proses manajemen keamanan informasi pada PDCA dapat dilihat melaui Tabel 2.1.

Tabel 2. 1 Peta PDCA dalam proses SMKI

PLAN *(adalah proses menetapkan Sistem Manajemen Keamanan Informasi)*	Pada proses ini dilakukan penetapan Sistem Manajemen Keamanan Informasi, terkait sasaran, prosedur, proses yang relevan untuk mengelola risiko dan meningkatakan keamanan informasi agar sesuai kebijakan dan sasaran organisasi.
DO (adalah proses menerapkan dan mengoperasikan *Sistem Manajemen Keamanan Informasi*)	Proses menerapakan dan mengoparasikan kebijakan dan aturan Sistem manajemen keamanan informasi juga terkait kontrol, proses dan prosedur – prosedur skeamanan informasi pada organisasi.
CHECK (adalah proses memantau dan melakukan tinjau ulang *Sistem Manajemen Keamanan Informasi*)	Pada proses ini kinerja prose diukur terhadap kebijakan, sasaran dan prakstek – praktek dalam menjalanakan Sistem Manajemen Keamanana Informasi, untuk selanjutnya dilapirkan kepada manajemen untuk ditindak lanjuti dan diperiksa efektifitasnya.
ACT (adalah proses memelihara dan melakukan peningkatan terhadap *Sistem Manajemen Keamanan Informasi*)	Proses terakhir pada siklus PDCA adalah melakukan Tindakan perbaikan sterhadap hasil evaluasiyang dilakukan oleh manajemen terkait dengan Sistem Manajemen Keamanan Informasi untuk tercapainya peningkatan yang berkelanjutan.

ISO 27000 Series terkenal sebagai *Information Security Management System* (ISMS) Familiy of Standards berisi tentang standar keamanan informasi. ISO 27000 didalamnya memuat : *Information technology, Security techniques, Information security management systems, Overview and vocabulary.* Standar tersebut dikembangkan oleh sub – *committee* 27 (SC27) dari *the first Joint Technical Committee* (JTC1) dari *International Organization for Standardization* dan *International Electrotechnical Commission.*

ISO 27000 mempunya beberapa fungsi diantaranya adalah sebagi berikut :

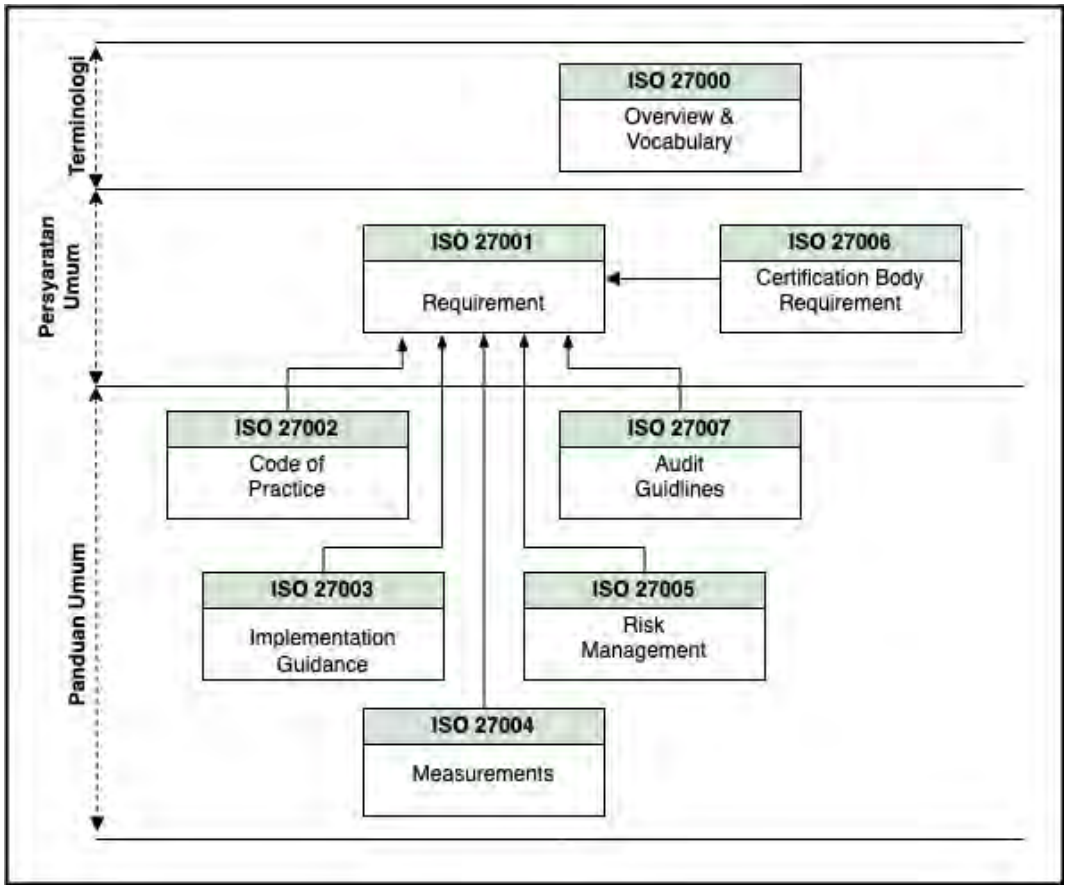
1. Memberikan gambaran dan pengenalan tentang *Information Security Management Systems* (ISMS) dari ISO 27000 *series*.
2. Memuat glossary atau kosa kata dari istilah dasar dan definisi yang digunakan dalam ISO 27000 series.

ISO mengelompokkan semua standar keamanan informasi ke dalam satu struktur penomoran, seperti pada serial ISO 27000.

Dari standar seri ISO 27000 ini, hingga September 2011, baru ISO/IEC 27001:2005 yang telah diadopsi Badan Standarisasi Nasional (BSN) sebagai Standar Nasional Indonesia (SNI) berbahasa Indonesia bernomor SNI ISO/IEC 27001:2009.

ISO 27001 adalah standar internasional yang berfokus pada proses bisnis dan aset bisnis, melakuakan pengurangan risiko terhadap data yang diangap berharga pada suatu organisasi. Stidaknya sampai akhir tahun 2017 terdapat 14000 perusahaan yang menggunakan standar ini dalam mengamankan sistem informasi yang mereka gunakan. Informasi yang dilindungi berupa keseluruhan innformasi yang berada pada organisasi tersebut baik yang berhubungan dengan IT maupun informasi yang tidak berhubungan dengan IT, juga informasi tersebut dapat berupa informasi digital maupun non digital semuanya dapat dilindungi oleh standar ISO 27001.

Berikut ini adalah hubungan antar standar dari keluarga ISO 27000 dapat dilihat pada Gambar 2.3 berikut :



Gambar 2. 3 Hubungan Antar Standar ISO 27000 series

Sumber : Direktorat keamanan Informasi 2011

Adapun beberapa standar di seri ISO ini adalah sebagai berikut:

1. ISO27000 : Dokumen definisi – definisi keamanan informasi yang digunakan sebagai istilah dasar dalam serial ISO 27000. Seri ini memberikan rekomendasi praktek terbaik atas manajemen keamanan informasi, risiko, dan kontrol dalam konteks keseluruhan *Information Security Management System* (Manajemen Keamanan Informasi Sistem), di desain untuk sistem manajemen jaminan mutu (ISO 9000 *series*) dan lingkup perlindungan (ISO 14000 *series*).
2. ISO27001 : Berisi aspek – aspek pendukung realisasi serta implementasi

sistem manajemen keamanan informasi perusahaan. Standar ISO 27001 diterbitkan pada bulan Oktober 2005, pada dasarnya menggantikan standar BS7799-2 yang sudah lama. Ini adalah spesifikasi untuk ISMS, suatu Sistem Manajemen Keamanan Informasi. BS7799 sendiri adalah sebuah standar yang sudah lama diterapkan, pertama kali diterbitkan pada tahun sembilan puluhan sebagai pedoman pelaksanaan. Bagian kedua muncul untuk menutupi sistem manajemen. Hal ini ditujukan terhadap sertifikasi yang diberikan.

3. ISO27002 : Isi dari ISO 27002 adalah terkait dengan ISO 27001, salah satu perbedaanya adalah pada dokumen ISO 27002 memuat dokumen berisi panduan terkait pelaksanaan dan implementasi Sistem Manajemen Keamanan Informasi organisasi. ISO 27002 awalnya bernama ISO 17799 (BS7799-1), yang berisi tentang pedoman untuk pelaksanaan keamanan informasi. ISO 27002 memuat ratusan kontrol yang dapat diimplementasikan kedalam teori.

4. ISO27003 : Panduan implementasi sistem manajemen keamanan informasi perusahaan. Tujuan dari pembangunan yang diusulkan adalah untuk memberikan bantuan dan bimbingan dalam melaksanakan ISMS (*Information Security Management System*). Ini akan mencakup fokus pada metode PDCA, sehubungan dengan penetapan, penerapan meninjau dan memperbaiki ISMS itu sendiri.

5. ISO27004 : Diterbitkan pada bulan Desember 2009, ISO 27004 menyediakan panduan dalam pengembangan dan penggunaan langkah – langkah, dan pengukuran dalam penilaian efektivitas dari penerapan dan kontrol sistem manajemen keamanan

informasi, sebagaimana telah ditentukan dalam ISO 27001. Lampiran dokumen juga menunjukkan metrik yang dipilih untuk menyesuaikan dengan ISO 27002.

Hal ini dimaksudkan untuk membantu organisasi menentukan efektivitas pelaksanaan ISMS-nya, merangkul pembandingan, dan kinerja penargetan dalam siklus PDCA.

Tujuan dari ISO/IEC 27004 adalah untuk membantu organisasi mengukur, melaporkan dan sistematis sehingga meningkatkan efektivitas mereka Sistem Manajemen Keamanan Informasi (SMKI).

6. ISO27005 : Dokumen panduan pelaksanaan manajemen risiko. ISO/IEC 27005 menyediakan pedoman untuk manajemen risiko keamanan informasi. Mendukung konsep – konsep umum yang ditetapkan dalam ISO/IEC 27001 dan dirancang untuk membantu pelaksanaan keamanan informasi berdasarkan pendekatan manajemen risiko.

7. ISO27006 : standar ini berisi tentang dokumen panduan untuk Sistem Manajemen Keamanan Informasi perusahaan. Ini adalah standar yang menawarkan panduan untuk akreditasi organisasi, yang menawarkan sertifikasi dan pendaftaran sehubungan dengan ISMS (*Information Security Management System*). Sekali lagi ini diawasi oleh komite ISO SC 27. Dengan standar sebelumnya yang terkait dengan masalah ini adalah EA 03/07. Ini secara efektif telah digantikan oleh standar baru, untuk memenuhi permintaan pasar untuk dukungan yang lebih baik bagi ISO 27001. Dokumen – dokumen merupakan hal yang efektif sebagai persyaratan tambahan yang diatur dalam ISO,

standar 17021 yang mengidentifikasi persyaratan yang lebih generik.

8. ISO27007 : ISO/IEC 27007 adalah bagian dari ISO/IEC Standar Sistem Manajemen Keamanan Informasi, di mana seri ISO/IEC 27000 merupakan standar keamanan informasi yang saat ini dikembangkan oleh Organisasi Internasional untuk Standarisasi (ISO) dan *International Electrotechnical Commission* (IEC).

2.5 ISO/IEC 27001:2013

ISO / IEC 27001 merupakan sebuah standar internasional yang mengatur tentang cara pengelolaan keamanan informasi. Pada awalnaya standar ini diterbitkan hasil kerjasama antara *the International Organisation for Standardization* (ISO) dan *the International Electrotechnical Commission* (IEC) pada tahun 2005 yang kemudian dikeluarkan versi terbarunya pada tahun 2013. ISO/IEC merinci persyaratan untuk menerapkan, menerapkan, dan terus meningkatkan sistem manajemen informasi (ISMS) yang bertujuan untuk membantu organisasi membuat aset informasi yang mereka miliki lebih aman.

Berikut ini adalah domain dan kontrol objektif yang terdapat pada ISO/IEC 27001:2013.

Tabel 2. 2 Kontrol Objektif ISO/IEC 27001:2013

	Domain (Klausul)	Kontrol Objektif
A.5	Kebijakan Keamanan Informasi	Untuk memberikan dukungan bagi organisasi terkait pengelolaan dan update kebijakan keamanan informasi menyesuaikan dengan regulasi yang berlaku.
A.6	Organisasi Keamaanan Informasi	Berfungsi untuk membuat kerangka kerja organisasi terkait pengendalian implementasi, serta operasi keamanan informasi pada organisasi.
A.7	Keamanan sumber daya manusia	Berfungsi untuk mengenali dan aset organisasi serta menetapakan tanggungjawab dan perlindungan terhadap aset tersebut sesuai dengan organisasi.
A.8	Manajemen Aset	Untuk mengidentifikasi aset organisasi dan menentukan tanggung jawab perlindungan yang sesuai.

Tabel 2. 3 Kontrol Objektif ISO/IEC 27001:2013 (lanjutan)

	Domain (Klausul)	Kontrol Objektif
A.7	Keamanan sumber daya manusia	Berfungsi untuk mengenali dan aset organisasi serta menetapakan tanggungjawab dan perlindungan terhadap aset tersebut sesuai dengan organisasi.
A.8	Manajemen Aset	Untuk mengidentifikasi aset organisasi dan menentukan tanggung jawab perlindungan yang sesuai.
A.9	Kontrol Akses	Membatasi akses informasi dan fasilitas pengolahan informasi.
A.10	Kriptografi	Untuk memastikan penggunaan kriptografi yang tepat dan efektif untuk melindungi kerahasiaan, keaslian dan / atau integritas informasi.
A.11	Keamanan fisik dan lingkungan	Untuk mencegah akses fisik yang tidak sah, kerusakan dan gangguan ke informasi organisasi dan fasilitas pemrosesan informasi.
A.12	Keamanan operasi	Untuk memastikan pengoperasian fasilitas pemrosesan informasi yang benar dan aman.
A.13	Keamanan komunikasi	Menjamin perlindungan informasi dalam jaringan dan sarana pemrosesan informasi pendukungnya.
A.14	Akuisisi, pengembangan dan pemeliharaan sistem	Untuk memastikan bahwa keamanan informasi merupakan bagian integral dari sistem informasi di seluruh siklus hidup. Ini juga mencakup persyaratan untuk sistem informasi yang menyediakan layanan melalui jaringan publik.
A.15	Hubungan pemasok	Untuk memastikan perlindungan aset organisasi yang dapat diakses oleh pemasok.
A.16	Information security incident management	Untuk memastikan pendekatan yang konsisten dan efektif untuk pengelolaan insiden keamanan informasi, termasuk komunikasi tentang kejadian dan kelemahan keamanan.
A.17	Aspek keamanan informasi dari manajemen kelangsungan bisnis	Kelangsungan keamanan informasi harus tertanam dalam sistem manajemen kelangsungan bisnis organisasi.
A.18	Kepatuhan	Untuk menghindari pelanggaran kewajiban hukum, undang-undang, peraturan atau kontrak yang terkait dengan keamanan informasi dan persyaratan keamanan apa pun.

Sumber : ISO/IEC 27001:2013

2.6 ISO/IEC 27001:2013 dan ISO/IEC 27002:2013

Pada bagian ini penulis akan menjelaskan tentang perbedaan ISO 27001 dan ISO 27002, serta menjelaskan perbandingan antara ISO 27002:2005 dengan ISO 27002:2013.

2.6.1. Perbedaan ISO 27001 dengan ISO 27002

Berkaitan dengan standar keamanan informasi IT, ISO 27001 bisa di bilang lebih familiar terdengan jika dibandingkan dengan ISO 27002 yang keduanya sama – sama diperuntukan untuk standarisasi keamanan informasi IT.

ISO 27002 adalah seperangkat standar dan prosedur yang berkaitan dengan keamanan dan kontrol informasi yang memungkinkan bisnis untuk menerapkan keamanan yang tepat. Standar ini sebagian besar dilengkapi dengan ISO 27001 yang merinci tugas manajerial seperti penilaian risiko dan meninjau keamanan. Dilain pihak, ISO 27002 banyak berbicara tentang aspek kontrol.

Dalam perkembangannya, sebelum munculnya ISO 27002 ada dua standar yang pernah digunakan yaitu standar BS7799, standar ini digunakan di negara Inggris, awal kemunculannya adalah pada tahun 1995. BS7799 kemudian diterbitkan ulang oleh ISO dan berganti nama menjadi ISO 17799. Pada tahun 2005 ISO 7799 disunting kembali dan berganti nama kembali menjadi ISO 27002. Meski telah berganti nama dan di sunting sebanyak dua kali, maun sama – sama digunakan sebagai standar untuk keamanan informasi.

ISO 27002 memuat ratusan cara untuk menangani keamanan informasi dan memiliki banyak bab tentang cara mengamankan informasi. Beberapa bab berkaitan dengan sumber daya manusia dan interaksi mereka dengan informasi, sementara yang lain memuat cara sebuah bisnis untuk mengontrol akses dan kelangsungan usaha dengan prosedur keamanan mereka. Keamanan informasi biasanya identik dengan teknologi informasi (TI), tetapi ISO 27002 juga berkaitan dengan mengamankan informasi diatas kertas, meskipun sebagian besar dari standar ini ditujukan untuk departemen TI.

ISO 27002 pada peluncuran pertamanya bertujuan untuk standarisasi semua organisasi yang membutuhkan keamanan isitem informasi. Ini berarti perusahaan, organisasi non-profit, lembaga pemerintah, dan entitas bisnis semua akan mengikuti standar yang sama. Namun, versi selanjutnya memisahkan standar untuk berbagai sektor agar lebih efisien. ISO 27002 berisi rincian tentang pengendalian dan prosedur yang

digunakan untuk menjaga informasi tetap aman. Standar lainnya, seperti ISO 27001, hanya berisi bagian kecil tentang kontrol. Sebaliknya, 27002 banyak berkaitan dengan kontrol tapi menawarkan sedikit dalam hal manajemen. Sebaliknya pada ISO 27001, semua aspek manajemen tersebut turut dimasukkan.

Sedangkan ISO 27001 bertujuan untuk memastikan keamanan informasi dan perlindungan data dalam organisasi di seluruh dunia. Standar ini sangat penting bagi organisasi bisnis dalam melindungi pelanggan mereka dan informasi rahasia organisasi terhadap ancaman. Penerapan sistem manajemen keamanan informasi akan memastikan kualitas, keamanan, layanan, dan keandalan produk dari organisasi yang dapat dijaga pada tingkat tertinggi.

Tujuan utama dari standar ini adalah untuk menyediakan persyaratan untuk menetapkan, menerapkan, memelihara dan terus meningkatkan Sistem Manajemen Keamanan Informasi (SMKI). Di sebagian besar perusahaan, keputusan untuk mengadopsi jenis standar ini diambil oleh manajemen puncak. Juga, persyaratan untuk memiliki sistem keamanan informasi semacam ini untuk organisasi muncul karena berbagai faktor seperti tujuan dan sasaran organisasi, persyaratan keamanan, ukuran dan samapai dengan struktur organisasi.

Dalam versi standar sebelumnya pada 2005, dikembangkan berdasarkan siklus PDCA, model *PLAN-DO-CHECK-ACT* untuk menyusun proses dan itu dengan cara mencerminkan prinsip – prinsip yang ditetapkan oleh pedoman OECG. Versi baru pada 2013 menekankan pada pengukuran dan evaluasi efektivitas kinerja organisasi dalam SMKI. Ini juga termasuk bagian yang didasarkan pada *outsourcing* dan lebih banyak konsentrasi diberikan untuk keamanan informasi dalam organisasi.

Persyaratan yang harus diterapkan untuk dokumentasi ISMS, dijelaskan dalam standar melalui penetapan konten penting, dokumen yang diperlukan serta spesifikasi dan struktur pemantauan untuk manajemen dokumen, seperti:

1. Proses perubahan dan persetujuan
2. Kontrol versi

3. Aturan untuk hak akses dan perlindungan akses
4. Spesifikasi untuk sistem pengarsipan

ISO 27001 dan 27002 menangani subjek yang sama, sehingga abanyak orang yang bingung membedakan perbedaan keduanya, alasam kedua standar itu di pisahkan dikarenakan apabila disatukan akan menghasilkan dokumen yang terlalu panjang dan membingungkan.

Kesimpulannya adalah ISO/IEC 27001 didalamnya memuat prasyarat untuk Sistem Manajemen Keamanan Inforamasi (SMKI), lain halnya dengan ISO/IEC 27002 yang didalamnya memuat pedoman dan prinsip – prinsip umum dalam pemeliharaan, penginisalisasian, dan perbaikan manajemen Sistem Manajemen Keamanan Informasi (SMKI) dalam sebuah organisasi. ISO/IEC 27001 didalamnya mencakup kebijakan keamanan, pengaturan dan klasifikasi aset, keamanan personil, keamanan fisik, manajemen operasi, kebijakan organisasi dan komunikasi sampai dengan manajemen keberlangsungan bisnis.

2.6.2. ISO/IEC 27002:2013

Jumlah kontrol pada ISO/IEC 27002:2013 berjumlah 114 kontrol, 35 keamanan utama yang tersebar dalam 14 domain, sedangkan pada ISO/IEC 27002:2005 jumlah kontrolnya sebanyak 133 kontrol yang tersebar pada 11 domain.

2.6.3. Domain ISO/IEC 27002:2013

Domain pada ISO/IEC 27002:2013 dimulai dari domain 5, hal ini terkait dengan sejarah ISO 27001. ISO 27001 pada awalnya adalah *British Standard* : BS ISO / IEC 17799: 2005 atau BS 7799-1: 2005.

British Standard menjadi Standar ISO untuk Sistem Manajemen. Bagian pertama dari ISO 27001 berkaitan dengan persyaratan untuk Sistem Manajemen. Persyaratan ("teknis") sebelumnya berasal dari BS digabungkan sebagai Lampiran A normatif (tidak informatif) dalam ISO 27001 baru menggunakan nomor yang sama A.5 -> A.15.

Penomoran klausul atau domain lama yaitu pada BS *(British Standard)* sampai saat ini masih di gunakan dalam ISO 27001 Annex A.

Sedangkan untuk penjelasan domain 1 sampai 4 secara singkat adalah sebagai berikut :

1. Domain A.0 : Pengantar

   Domain ini berisikan pengantar atau epengenalan terkait ISO 27002:2013. Selain itu juga dijelaskan tentang latar belakang dan konteks, persyaratan keamanan informasi, pemilihan kontrol, pengembangan pedoman *(guidlines)* sendiri, pertimbangan siklus hidup, dan standar terkait.

2. Domain A.1 : Cakupan

   Praktik manajemen keamanan informasi termasuk didalamnya mengenai pemilihan, implementasi dan manajemen pengendalian dengan mempertimbangkan lingkungan risiko keamanan informasi organisasi. Standar ini dirancang untuk digunakan oleh organisasi dengan tujuan untuk :

   a. Memilih kontrol dalam proses penerapan Sistem Manajemen Keamanan Informasi berdasarkan ISO/IEC 27001;
   b. Menerapkan kontrol keamanan informasi yang diterima secara umum;
   c. Mengembangkan pedoman manajemen keamanan informasi mereka sendiri.

3. Domain A.2 : Acuan normative

   Dokumen – dokumen berikut (ISO 27002:2013), sebagian atau keseluruhan, secara normatif dirujuk dalam dokumen ini, juga sangat diperlukan dalam proses penerapannya.

4. Domain A.3 : Istilah dan definisi

   Pada dokumen ini, istilah dan definisi yang dipakai adalah mengacu ISO/IEC 27000.

5. Domain A.4 : Penjelasan struktur

Setiap klausul yang mendefinisikan kontrol keamanan berisi satu atau lebih kategori keamanan utama. Urutan klausul dalam standar ini tidak menyiratkan kepentingannya. Bergantung pada situasinya, kontrol keamanan dari salah satu atau semua klausul mungkin penting, oleh karena itu setiap organisasi menerapkan ini standar harus mengidentifikasi pengendalian yang dapat diterapkan, seberapa penting hal ini dan penerapannya bagi individu proses bisnis. Selain itu, daftar dalam standar ini tidak berada dalam urutan prioritas. Setiap kategori kontrol keamanan utama berisi:

1. Tujuan pengendalian yang menyatakan apa yang ingin dicapai;
2. Satu atau lebih pengendalian yang dapat diterapkan untuk mencapai tujuan pengendalian.

Deskripsi kontrol disusun untuk mendefinisikan pernyataan pengendalian khusus, untuk memenuhi tujuan pengendalian. Sedangkan untuk panduan implementasinya adalah memberikan informasi yang lebih detail untuk mendukung pelaksanaan pengendalian dan pemenuhan tujuan pengendalian. Panduan tersebut mungkin tidak sepenuhnya sesuai atau cukup di semua situasi dan mungkin juga tidak memenuhi persyaratan kontrol khusus organisasi. .

Selain pada penjelasan diatas, sebagai tambahan informasi lain adalah untuk memberikan informasi lebih lanjut yang mungkin perlu dipertimbangkan, misalnya pertimbangan hukum dan referensi ke standar lain. Jika tidak ada informasi lain yang akan diberikan, bagian ini tidak akan ditampilkan.

Isi pada domain A.1 sampai dengan A.4 adalah tentang penjelasan atau gambaran umum mengenai ISO/IEC 27002:2013. Juga menjelaskan secara singkat aturan pada ISO 27002:2013. Berikut ini adalah domain yang terdapat pada ISO/IEC 27002:2013 :

Tabel 2. 4 Domain ISO/IEC 27002:2013

Domain	*Control*	*Objective*
A.5	*Information security policies*	*To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.*
A.6	*Organization of information security*	*To ensure the security of teleworking and use of mobile devices.*
		To ensure the security of teleworking and use of mobile devices.
A.7	*Human resource security*	*To ensure that employees and contractors are aware of and fulfil their information security responsibilities.*
		To ensure that employees and contractors are aware of and fulfil their information security responsibilities.
A.8	*Asset management*	*To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.*
		To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.
		To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.
A.9	*Access control*	*To limit access to information and information processing facilities.*
		To ensure authorized user access and to prevent unauthorized access to systems and services.
		To make users accountable for safeguarding their authentication information.
		To prevent unauthorized access to systems and applications.
A.10	*Cryptography*	*To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.*
A.11	*Physical and environmental security*	*To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.*
		To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.
A.12	*Operations security*	*To ensure correct and secure operations of information processing facilities.*
		To ensure that information and information processing facilities are protected against malware.
		To protect against loss of data.
		To record events and generate evidence.
		To ensure the integrity of operational systems.
		To prevent exploitation of technical vulnerabilities.
		To minimise the impact of audit activities on operational systems.

Tabel 2. 5 Domain ISO/IEC 27002:2013 (lanjutan)

Domain	*Control*	*Objective*
A.13	*Communications security*	*To ensure the protection of information in networks and its supporting information processing facilities.*
		To maintain the security of information transferred within an organization and with any external entity.
A.14	*System acquisition, development and maintenance*	*To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.*
		To ensure that information security is designed and implemented within the development lifecycle of information systems.
		To ensure the protection of data used for testing.
A.15	*Supplier relationships*	*To ensure protection of the organization's assets that is accessible by suppliers.*
A.16	*Information security incident management*	*To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.*
		To maintain an agreed level of information security and service delivery in line with supplier agreements.
A.17	*Information security aspects of business continuity management*	*Information security continuity should be embedded in the organization's business continuity management systems.*
		To ensure availability of information processing facilities.
A.18	*Compliance*	*To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.*
		To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

Sumber : ISO/IEC 27002:2013

2.6.4. Perbedaan ISO 27002:2005 dengan ISO 27002:2013

ISO/IEC 27002:2013 adalah standar yang identik dengan ISO/IEC 27002:2005, yang menetapkan pedoman dan prinsip – prinsip umum untuk memulai, melaksanakan, memelihara, dan meningkatkan manajemen keamanan informasi dalam suatu organisasi. Tujuan dari standar ISO/IEC 27002:2013 adalah untuk memberikan penjelasan mengenai panduan umum mengenai diterimanya tujuan umum manajemen keamanan informasi.

Perbedaan terbesar antara ISO/IEC 27002:2005 dengna ISO/IEC 27002:2013 adlah terkait dengan struktur didalamnya. ISO/IEC 27002 2005 memiliki 11 klausul (klausul 5 sampai dengan 14), sementara itu ISO/IEC 27002:2013 memiliki 14 klausul (klausul 5 sampai dengan klausul 18). Klausul baru pada ISO/IEC 27002:2013 adalah klausul 10, 13, dan 15 yaitu terkait dengan kriptografi, keamanan komunikasi dan hubungan dengan pemasok, sebagaimana terlihat dalam Gambar 2.4, berikut ini :

Gambar 2. 4 Skema Kontrol Objektif ISO 27002:2013

Sumber : ISO 27002:2013

Pada gambar diatas dijelaskan bahwa bagian membahas kriptografi, keamanan komunikasi, dan hubungan pemasok (bagian 10, 13, dan 15 masing-masing). Namun, sementara standar baru memiliki tiga bagian yang lebih, itu adalah sebenarnya lebih pendek dan lebih fokus daripada yang lama.

Standar lama memiliki 106 halaman konten 25 sementara yang baru hanya memiliki 78. ISO/IEC 27002:2013 juga memiliki sub bagian klausul baru yaitu seubbagian 6.1.5 berisi tentang keamanan manajemen proyek, 8.2.3 berisi tentang penanganan aset, 12.6.2 membahas tentang instalasi perangkat lunak, 14.2.1 membahas tentang keamanan

pengembangan, 14.2.6 membahas keamanan pengembangan lingkungan, 14.2.8 membahas tentang pengujian sistem, 15.1.1, 15.1.2, dan 15.1.3 ketiganya membahas tentang keamanan pemasok, 16.1.4 berisi tentang penanganan peristiwa keamanan, 17.1.1, 17.1.2, dan 17.1.3 berisi tentang perencanaan, pelaksanaa, dan verifikasi keberlangsungan keamanan informsi, dan yang terakhir adalah subkalusul 17.2.1 terkait penggunaan fasilitas pemrosesan informasi yang berlebihan. Selain perbedaan yang telah disebutkan diatas, Sebagian besar dari klausul pada ISO/IEC 27002:2013 telah ditulis ulang, dan beberapa bagaian klausul telah diposisikan ulang dan berpindah ke bagian lain.

ISO 27002: 2005 berisi panduan yang menjelaskan contoh penerapan keamanan informasi dengan menggunakan bentuk-bentuk kontrol tertentu agar mencapai sasaran kontrol yang ditetapkan.Bentuk-bentuk kontrol yang disajikan seluruhnya menyangkut 11 area pengamanan sebagaimana ditetapkan didalam ISO/IEC 27001. Sarno dan Iffano (2009: 187) mengatakan kontrol keamanan berdasarkan ISO/IEC 27001 terdiri dari 11 klausul kontrol keamanan *(security control clauses),* 39 objektif kontrol *(control objectives)* dan 133 kontrol keamanan atau kontrol *(controls)* yang dapat dilihat dalam berikut :

Tabel 2. 6 Domain, kontrol objektif dan kotrol pada ISO27002:2005

Domain	Jumlah	
	Objektif Kontrol	Kontrol keamanan
A.5	1	3
A.6	2	11
A.7	2	5
A.8	3	9
A.9	2	13
A.10	10	31
A.11	7	25
A.12	6	16
A.13	2	5
A.14	1	5
A.15	3	10
Jumlah		
11	39	133

Sumber : ISO27002:2005

2.7. CMMI *(Capability Maturity Model Integration)*

Pada penelitian ini dilakukan perhitungan tingkat kematangan menggunakan *Capablity Maturity Model Integration* (CMMI).

Capability Maturity Model Integration (CMMI) merupakan sebuah model peningkatan proses, tujuannya adalah membantu organisasi dalam usaha meningkatkan kinerja. Didalam CMMI terdiri dari kumpulan *best practices* yang menggambarkan karakteristik dari sebuah peningkatan proses efektif. Pada awal kemunculannya Pada tahun 1987 di Pittsburgh CMMI dikembangkan oleh SEI *(Software Engineering Institut)* dan dikenal dengan nama CMM atau *Capability Maturity Model* dikembangkan oleh SEI *(Software Engineering Institut),* yang selanjutnya dikenal dengan CMMI.

CMMI memungkinkan organisasi melakukan proses penilaian secara bertingkat, penilaian tersebut berdasarkan dari kuisioner yang dikembangkan secara khusus untuk perangkat lunak.

Berikut ini adalah kegunaan CMMI bagi organisasi :

1. Mengukur tingkat kematangan dari suatu perusahaan pengembang *software.*
2. Alat bantu *benchmarking* dengan organisasi lain.
3. Memberikan arahan bagi *top management* dalam usaha peningkatan kinerja pada sebuah organisasi.
4. Dengan penerapan CMMI, organisasi dapat menekan pengeluaran biaya, meningkatkan mutu dan menghemat waktu pengerjaan suatu proyek.

CMMI dengan kata lain merupakan sebuah kerangka yang berfungsi untuk mengembangkan proses, proses yang dimaksud adalah seperti proses teknis, baik proses teknis formal atau informal. Sedangkan pembobotan yang dilakukan adalah hasil adopsi dari penilaian risiko.

Dalam hubungannya dengan Sistem Manajemen Keamanan Informasi (SMKI), risiko merupakan dampak yang ditimbulakan atas terjadinya suatu hal yang dapat mengancam keamanan informasi pada sebuah organisasi, sedangkan ancaman yang dimaksud adalah yang berhubungan dengan aspek CIA *(Confidentiality, Integrity dan Availability).*

Capability Maturity Model Integration atau CMMI terdiri dari dua bagian, yaitu:

1. Model untuk teknik keamanan proses, proyek dan organisasi, dan

2. Metode penilaian untuk mengetahui kematangan proses.

Versi pertama dari CMMI dikeluarkan pada bulan Oktober 1996. Pada tahun CMMI menjadi standar ISO/IEC 21827. CMMI sendiri terdiri dari tiga versi, and versi terbaru dikeluarkan pada Juni 2003.

CMMI mempunyai tingkat pengukuran kematangan, seperti yang dapat dilihat pada Tabel 2.4 berikut ini :

Tabel 2. 7 Kriteria indeks penilaian pada tingkat kematangan

Skor (Skala)	Status	Keterangan
0 – 0.50	*Non-existient*	*Management Processes are not applied at all*
0.51 – 1.50	*Initial*	*Processes are ad hoc and disorganized*
1.51 – 2.50	*Repeatable*	*Processes follow a regular pattern*
2.51 – 3.50	*Defined*	*Processes are documented and communicated*
3.51 – 4.50	*Managed*	*Processes are monitored and measured*
4.51 – 5.00	*Optimised*	*Good practices are followed and automated*

Penjelasan dati Tabel 2.4 :

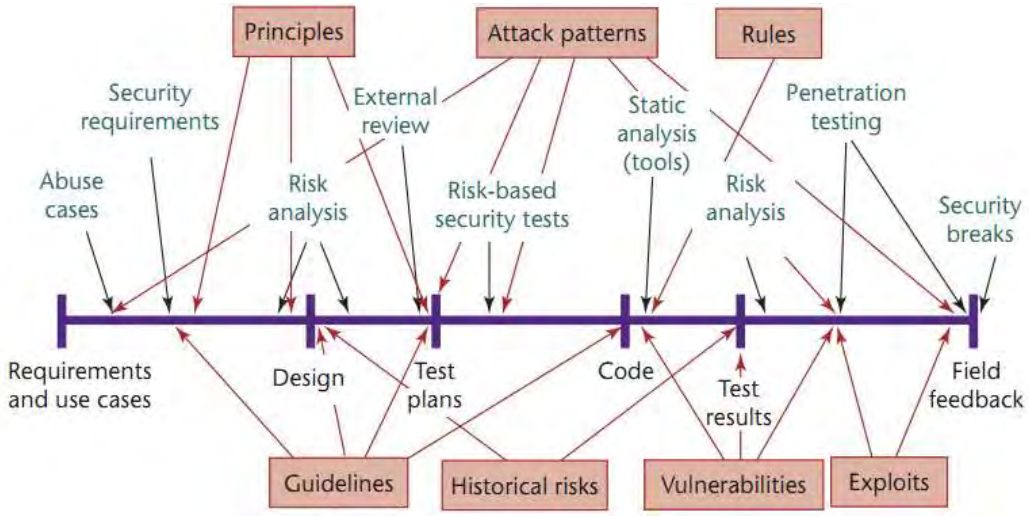
1. Tingkat 0 Tidak semua praktek dasar dilakukan.
2. Tingkat 1 Semua praktek dasar dilakukan namun secara informal, yang artinya tidak ada dokumentasi, tidak ada standar dan dilakukan secara terpisah.
3. Tingkat 2 *Planned* dan *tracked* yang menandakan komitmen merencanakan proses standar.
4. Tingkat 3 *Well defined* yang berarti proses standar telah berjalan sesuai dengan definisi.
5. Tingkat 4 Dikendalikan secara kuantitatif, yang berarti peningkatan kualitas melalui monitoring setiap proses.
6. Tingkat 5 Ditingkatkan terus-menerus yang menandakan standar telah sempurna dan fokus untuk beradaptasi terhadap perubahan.

2.6 Keamanan Piranti Lunak

Keamanan piranti lunak adalah sebuah proses mendesain, membuat kemudian melakukan tes kepada software tersebut dengan memeperhatikan tingkat keamanan dari setiap bagian supaya software tersebut dapat menahan serangan (G. McGraw, 2006).

Piranti lunak yang aman bergantung pada proses rekayasa, bahasa pemrogmana yang dipilih dan teknik pengamaman yang digunakan untuk melindungi piranti lunak. Membangun piranti lunak yang aman dan tanpa kelemahan adalah sebuah kemustahilan untuk dilakukan, keamananan piranti lunak dapat ditembus oleh berbagai cara, hanya permasalahan waktu, kesempatan dan cara bagi seorang penyerang untuk dapat menemuakan kelemahan dan menembus keamanan piranti lunak yang dibangun.

Meskipun membangun piranti lunak yang aman tidak mungkin dilakukan, hal yang dapat dilakukana dalah dengan meningkatkan kesadaran akan keamanan piranti lunak sejak piranti lunak itu mulai dibangun. Tiga pilar utama keamanan software yaitu pengetahuan, manajemen risiko dan *touchpoint*. Menerapkan ketiganya dalam pembangunan software secara bertahap dan sesuai dengan ketentuan maka akan di dapat software yang sesuai dengan standar dan hemat. Menurut Gary McGaw, tahapan pembangunan software dengan penerapan tigapilar tersebut adalah sebagai berikut :



Gambar 2. 5 Tahapan Secure Software Development Life Cycle (SDLC)

(Sumber : "*Software security*", G. McGraw, IEEE *security & privacy*)

Setiap potensi risiko keamanan software dapat memberikan dampak yang berbeda bagi pengguna piranti lunak, sehingga setiap potensi risiko kemanan tersebut harus diperhatikan. Gambaran risiko kemanan dan dampaknya terhadap pengguna software dapat dijelaskan dalam Gambar 2.6 berikut:

Gambar 2. 6 Potensi serabgan dan dampaknya

Sumber :

Dengan diketahuinya dampak dari suatu serangan keamanan pada software, maka langkah – langakah preventif pun dapat dilakunan sedari awal sebelum dampak kerusakan yang ditimbulkan tidak terlalu besar.

2.9 Skala Guttman

Skala Guttman dibuat dan dikembangkan oleh Louis Guttman. Skala ini memiliki ciri penting, yaitu skala ini merupakan skala kumulatif dan digunakan untuk mengukur satu dimensi saja dari satu variable yang multi dimensi, sehingga skala ini termasuk mempunyai sifat undimensional. Skala ini juga disebut dengan metode Scalogram atau analisa skala *(scale analysis)*. Skala Guttman sangat baik untuk meyakinkan peneliti tentang kesatuan dimensi dari sikap atau sifat yang diteliti, yang sering disebut isi universal (universe of content) atau atribut universal *(universe attribute)*. Sebagai mana skala *Thurstone*, pernyataan – pernyataan memiliki bobot yang berbeda, dan jika responden menyetujui pernyataan yang memiliki bobot lebih berat, maka diharapkan akan menyetujui pernyataan yang berbobot lebih rendah.

Untuk menilai undimensionalnya suatu variable pada skala ini, diadakan analisis skalogram untuk mendapatkan koefisien reproduksibilitas (Kr), dan koefisien skalabilitas (Ks), dimana jika nilai Kr = ≥ 0,90 dan Ks = ≥ 0,60 skala dianggap bagus (layak).

Tujuan Guttman menggunakan skala ini adalah untuk mengetahui atau menetapkan apakah sikap yang sedang diselidiki itu benar – benar hanya menyangkut satu dimensi saja. Suatu sikap dianggap berdimensi tunggal hanya jika sikap itu menghasilkan skala kumulatif, yaitu skala yang butir – butirnya berkaitan satu sama lain sehingga seorang subjek yang setuju dengan 30 pernyataan nomor 2, akan juga setuju dengan pernyataan nomor 1; subjek yang setuju dengan nomor 3, maka akan juga setuju dengan pernyataan nomor 1 dan 2; dan seterusnya. Jadi seseorang yang menyetujui pernyataan tertentu dalam skala ini akan mempunyai skor skala keseluruhan yang lebih tinggi daripada orang yang tidak menyetujui pernyataan tersebut.

Menurut (Sugiyono, 2011), skala Guttman adalah skala yang digunakan pada jawaban yang mempunyai sifat jelas atau tegas. Contohnya seperti ya – tidak; setuju – Tidak setuju; benar – ; pernah – belum pernah; positif – negative dan sebagainya.

2.10 Analisa Kesenjangan

Gap Analysis adalah metode untuk membandingkan kineja eksisting (yang sedang terjadi) dengan kinerja harapan atau potensial. Metode ini menitikberatkan pada evaluasi bisnis pada kesenjangan kinerja organisasi eksisting dengan kinerja target. Gap Analisis juga berfungsi untuk mengidentifikasi langakah atau tinndakan yang harus dilakukan untuk dapat mengurangi gap atau kesenjangan supaya didapat kinerja sesuai tujuan yang diharapkan.

Gap analisis juga dapat menghasilakan perkiraan biaya, waktu dan sumberdaya lainnya yang diperlukan dalam usaha mencapai kondisi yang ideal atau yang diharapkan.

2.11. Penelitan sebelumnya

Marliana Halim, dalam karya ilmiahnya yang diberi judul Audit Keamanan Informasi Berdasarkan Standar ISO 27002 dimana sudah dipublikasikan dalam jurnal JSIK, Vol.1 2012 mengatakan bahwa penyalahgunaan password diakibatkan karena organisasi tidak mengatur dan kurang tegas terhadap perlindungan, kerahasiaan, dan pengamanan password, selanjutnaya perusahaan juga tidak menekankan kepada karyawan untuk dapat mengamankan dan menjaga kerahasiaan password masing masing karyawan.

Febrianto, Febri dalam jurnal AMIK JTC INFOKAM yang dipublikasikan pada Vol.14 No 1 2020 menyimpulkan bahwa STMIK Tunas Bangsa setelah diaudit memiliki tingkat kematangan sebesar 2,6 hal itu menunjukan bahwa sudah ada pengelolaan informasi, hanya saja terdokumentasi dan belum melakukan prosedur keamanan sesuai dengan pedoman yang baku atau belum mengacu pada suatu standar, semua kegiatan hanya berdasarkan kebiasaan. Dengan demikian, pengelolaan informasi di STIMIK Tunas Bangsa masih memerlukan perbaikan untuk memastikan keamanan informasi terjaga dengan baik.

Winda Apriandari , dalam karya ilmiahnya yang beri judul Alisis Sistem Manajemen Keamanan Informasi Menggunakan SNI ISO/SEC 27001:2013 pada pemerintahan daerah Kota Sukabumi yang di publikasikan pada jurnal ilmiah SANTIKA Vol.8 No.1 tahun 2018 setelah dilakukan analisa dan perhitungan dari 25 prfil risiko menemukan 1 risiko bersifat crical, 6 risiko bersifat medium dan sisanya 17 risiko bersifat rendah atau low, sedangkan untuk perhitungan kematangan didapat rata rata nilai 2.00. kesimpulannya dalah tidak adanya standar yang digunakan dalam penerapan sistem informasi menyebabkan munculnya risiko keamanan yang dapat mengganggu kelancaran berjalannya sitem informasi.

Rokhman Fauzi dalam penelitiannya yang berjudul Implementasi Awal Sistem Manajemen Informasi pada UKM Menggunakan Kontrol ISO/IEC 27002 yang telah di terbitkan pada Journal Teknologi Rekayasa (JTERA) Vol. 3, No. 2 Desember 2018.

Penelitian tersebut menggunakan kontrol ISO/IEC 27002 dan metode OCTAVE-S, penelitian ini menunjukan dengan tidak diterapkannya suatu standar pada perusahaan menunjukan bahwa perusahaan memiliki risiko keamanan tingkat sedang (medium). Maka dilakukanlah mitigasi keamanan. Mitigasi awal dilakukan pada area kontrol: kebijakan keamanan informasi, keamaman sumberdaya manusia, keamanan fisik dan lingkungan, komunikasi dan manajemen operasi, kontrol akses, dan manajemen insiden keamanan informasi. Hal tersebut dilakukan untuk menanggulangi kemungkinan terjadinya risiko keamanan yang dapat terjadi pada organisasi atau perusahaan.

Desak made Novita dalam penelitiannya yang berjudul Mengetahui tingkat kematangan aplikasi pada *start up IT* menggunakan metode CMMI dan TMMi menemukan bahwa metode tersebut dapat mengukur dan mengetahui tingkat kematangan dari team startup IT, Hasil yang diketahui dengan metode tersebut adalah terdapat 11 team start up masih berada pada maturity level 2 Managed. Proses yang dicapai diantaranya adalah REQM (6 *team*), PP (4 *team*), PMC (6 *team*), SAM (1 *team*), PPQA (5 *team*) dan CM (2 *team*). Dari penelitia tersebut didapatkan hasil yang dapat digunakan sebagai bahan acuan pengambilan keputusan bagi peneliti ataupun instansi yang memerlukan.

Tabel 2. 8 Susunan penelitian yang telah dilakukan

No	Paper Utama	Manajemen Keamanan Informasi	Framework	Pengujian
1.	Marliana Halim / 2012	ISO 27002	COBIT 4.1	Audit keamaman sistem informasi pada perusahaan untuk mengukur tingkat kematangan pada sistem informasi eksisting.
2.	Ferry Febrianto / 2017	ISO 27002	-	Evaluasi keamanan informasi pada STMIK Tunas Bangsa untuk mengetahui tingkat keamanan dengan pengukuran maturity model pada sistem eksisting, untuk dijadikan rujukan perbaikan dimasa mendatang.
3.	Winda Apriandari / 2018	ISO 27001	CMMI	Melakukan analisis terhadap keamanan sistem informasi menggunakan kontrol ISO 27001 untuk mengidentifikasi masalah kebutuhan user, studi kelayakan, evaluasi pemelihataan dan penerapan sistem informasi.

Tabel 2. 9 Susunan penelitian yang telah dilakukan (Lanjutan)

No	Paper Utama	Manajemen Keamanan Informasi	Framework	Pengujian
4.	Rokhman Fauzi / 2018	ISO 27002	OCTAVE-S	Implementasi awal sistem manajemen keamanan informasi menggunakan kontrol ISO 27002 untuk melakukan mitigasi dan untuk menemukan kemungkinan terjadinya risiko keamanan informasi.
5.	Desak Made Novita / 2019	-	CMMI - TMMi	Penelitian ini dapat mengetahui tingkat kematangan menggunakan metode CMMI dan TMMi untuk mengetahui tingkat kematangan dari 11 team startup IT.

BAB III

METODOLOGI PENELITAIN

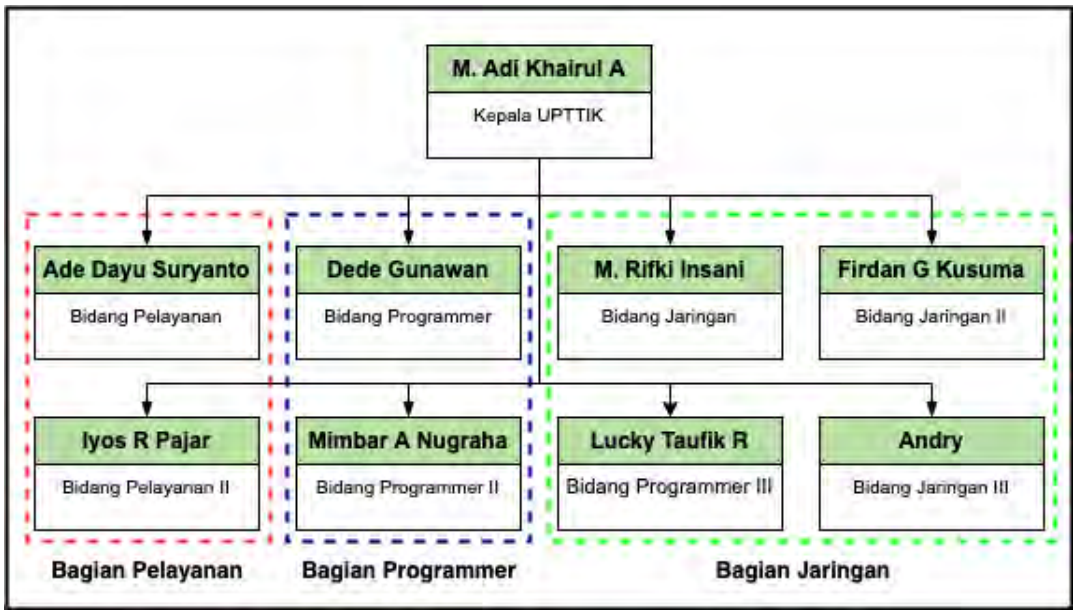
3.1 Profil UPTTIK

Unit Pelayanan Teknologi Informasi dan Komunikasi (UPTTIK) Universitas Siliwangi adalah unit yang berada di Universitas Siliwangi yang bertugas dan bertanggungjawab mengelola hampir seluruh sistem informasi yang ada di Universitas Siliwangi. Anggota UPTTIK Universitas Siliwangi berjumlah delapan orang anggota, kedelapan anggota dibagi kedalam tiga kelompok tugas, yaitu bidang *networking*, bidang *programmer* dan bidang pelayanan.

Tugas dan fungsi bidang sebagai berikut :

1. Bidang *networking* bertugas untuk mengurusi masalah jaringan, termasuk pemasangan *access point,* pemasangan CCTV, installasi dan konfigurasi *server*, samapai dengan pemeliharaan perangkat jaringan dan *server*.
2. Bidang *programmer* bertugas pada pembuatan dan pengembangan sistem informasi, sampai perawatan sistem informasi.
3. Bidang pelayanan bertugas menerima segala bentuk keluhan dari pengguna jaringan dan sistem informasi yang dikelola oleh UPTTIK Universitas Siliwangi, juga memberikan pelatihan – pelatihan penggunaan sistem informasi kepada dosen, mahasiswa dan karyawan Universitas Siliwangi.

Berikut ini adalah gambar struktur organisasi UPTTIK Universitas Siliwangi :



Gambar 3. 1 Struktur Organisasi UPTTIK

Sumber : UPTTIK Universitas Siliwangi

Ketiga bidang tersebut diatur oleh seorang kepala unit, kepala unit adalah merupakan dosen dengan tugas tambahan, yaitu seorang dosen yang di tugaskan dengan tugas tambahan seperti menjadi kepala atau pimpinan pada suatu unit yang berada di Universitas Siliwangi.

UPTTIK Universiatas Siliwangi merupakan suatu unit yang bertanggungjawab secara langsung kepada Rektor Universiatas Siliwangi dalam menajalankan tugas dan fungsinya.

3.2 Denah UPTTIK

UPTTIK berada di lantai dua gedung rektorat Universitas Siliwangi, lokasinya berdampingan langsung dengan ruang serbaguna yang juga berfungsi sebagai ruang rapat utama Universitas Siliwangi. Ruangan UPTTIK dibagi menjadi tiga ruangan utama, yaitu ruangan 1 (ruang karyawan), ruang 2 (ruangan pimpinan) yang merangkap sebagai ruang rapat UPTTIK, dan ruangan 3 (ruangan *server*) menyatu dengan ruang jaringan atau

network. Ruang *server* aplikasi SIMAK berdampingan langsung dengan ruang rapat, dipisahkan oleh sekat dinding kaca permanen.

Ruangan *server* pada UPTTIK dalam perancangannya belum memakai standar keamanan yang diperuntukan untuk ruangan *server*, hal ini dikarenakan UPTTIK masih menggunakan bangunan lama yang diperuntukan untuk kantor pada umumnya. Seperti yang dapat dilihat pada gambar 3.2, meski ruang *server* sudah di amankan menggunakan akses kunci sidik jari, namun pada sekeliling ruang *server* ada bagian yang hanya dibatasi atau menggunakan dinding kaca yang mudah di tembus atau dipecahkan. Pemakaian ruangan yang tidak mengikuti atau tidak menggunakan standar keamanan untuk ruangan *server* ini dapat memicu permasalahan, diantaranya adalah permasalahan keamanan, permasalahan keamanan yang dimaksud adalah yang timbul dari internal ataupun eksternal.

Berikut ini adalah gambaran sederhana mengenai denah UPTTIK secara keseluruhan :

Gambar 3. 2 Denah ruangan UPTTIK

Sumber : UPTTIK Universitas Siliwangi

Penjelasan gambar :

1. Ruangan 1 (Ruang karyawan)

   Dapat diakses dengan satu akses utama dan diamankan menggunakan kunci pintu konvensional (belum menggunakan kunci elektronik), ruang 1 dapat dakses oleh semua orang. Pada ruang 1 terdapat juga ruangan yang diperuntukan sebagai gudang penyimpanan barang UPTTIK, empat karyawan bekerja pada ruangan 1, ruang 1 juga adalah akses satu satunya untuk dapat masuk ke ruang 2. Pada ruang 1 terdapat satu akaryawan yang juga berperan sebagai resepsionis. Pada ruang 1 tamu dilayani sesuai dengan keperluannya masing – masing. Tamu yang masuk hanya bisa sampai ke ruang 1 dan apabila mempunyai keperluan ke ruang 2 atau ruang 3 harus dengan seizin dan di damping oleh karyawan UPTTIK.

2. Ruangan 2 (Ruang karyawan)

   Pada ruangan 2 tidak semua orang dapat masuk ke area ini, hanya karyawan yang sudah mempunyai hak akseslah yang dapat masuk ke ruangan ini, hal ini dikarenakan ruangan 2 telah diamankan oleh kunci sidik jari. Pada ruangan 2 terdapat dua orang karyawan, satu orang karyawan yang bertugas sebagai *server* dan *network engineer* dan kepala UPTTIK. Ruangan 2 bersebelahan langsung dengan ruangan 3 dan dibatasi oleh pembatas atau jendela kaca permanen. Pada ruanngan 2 juga terdapat satu akses untuk menuju ke ruangan *server*. Ruangan 2 bersebelahan langsung dengan ruang serbaguna, dibatasi oleh jendela kaca permanen.

3. Ruangan 3 (Ruang *server*)

   Ruangan ini sebenarnya adalah ruangan inti dari ketiga ruangan yang ada di UPTTIK, dimana ruangan ruangan 3 adalah ruangan yang berisi *rack server* juga *rack network* atau jaringan, untuk dapat masuk atau mengakses ruangan ini lebih ketat lagi jika dibandingkan dengan ruangan 1 dan ruangan 2, tidak semaua karyawan UPTTIK yang dapat masuk ke ruangan 3, hanya beberapa orang saja dari karyawan UPTTIK yang dapat masuk ke ruangan 3. Hal ini dikarenakan pada

ruangan 3 terdapat lebih dari 25 *server* dan jaringan termasuk didalamnya adalah *server* aplikasi SIMAK berada. Sama halnya dengan ruangan 2, ruangan 3 juga bersebelahan dengan ruang serbaguana dan hanya di batasi oleh jendela kaca permanen, terkait dengan keamanan, hal ini sangat berbahaya mengingat orang yang tidak bertanggungjawab bisa masuk dengan cara memecahkan kaca pembatas antara dua ruangan tersebut.

3.3 Aplikasi SIMAK

SIMAK adalah kepanjangan dari Sistem Informasi Akademik merupakan salah satu aplikasi yang dikelola oleh UPTTIK Universiitas Siliwangi, salah satu fungsi utamanya adalah untuk mengolah data akademik seperti data mahasiswa, kontrak matakuliah, penilaian matakuliah, penjadwalan matakuliah, registrasi perkuliahan, sampai dengan pengelolaan pembayaran perkuliahan.

Server aplikasi SIMAK berada pada ruangan 3 (lihat denah UPTTIK) yaitu ruangan *server* utama UPTTIK. Untuk dapat mengakases *server* aplikasi SIMAK terlebih dahulu harus melewati ruangan 2 yang dibatasi oleh fitur keamanan berupa kunci sidik jari.

Pada paraktek penggunaanya aplikasi SIMAK dikelola oleh berbagai level akses, mulai dari akses utama (administrator), yaitu *admin* UPTTIK, *level admin* fakultas, program studi, sampai pengguna akhir yaitu mahasiswa, semuanya mempunyai hak akses dan wewenang yang berbeda terkait dengan pengelolaan aplikasi SIMAK tersebut.

Aplikasi SIMAK pertamakali dibangun pada tahun 2010, yaitu pengembangan dari aplikasi *opensource* SISFO kampus, seiring bertambahnya kebutuhan data dan informasi, maka banyak modul yang disesuaikan atau di tambah disesuaikan dengan kebutuahan Universitas Siliwangi.

Lengkapnya fitur dan fungsi yang dimiliki oleh aplikasi SIMAK, juga besarnya data yang diolah didalamnya ternyata tidak diikuti oleh penerapan standar keamanan informasi terutama terkait dengan *Confidentiality, Integrity dan Avalilability.* Hal ini tentu dapat

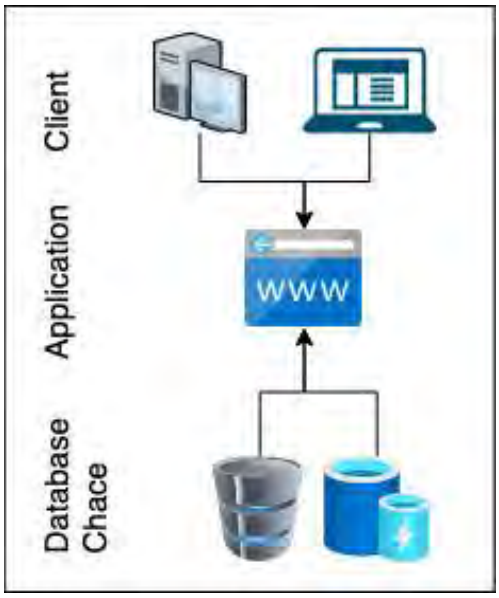
membahayakan kelancaran dan keberlangsungan proses kerja dari aplikasi SIMAK itu sendiri.

Ancaman yang mungkin muncul yang disebabkan belum diterapkannya standarisasi pada keamanan di UPTTIK khususnya pada aplikasi SIMAK adalah terkait dengan keamanan data.

3.3.1. Infrastruktur Aplikasi SIMAK

Infrastruktur aplikasi SIMAK diartikan sebagai sumberdaya teknologi yang menopang berjalannya aplikasi SIMAK, sehingga dapat berjalan dan dapat digunakan dengan baik. Infrastruktur aplikasi simak dibagi menjadi dua kelompok yaitu infrastruktur software dan hardware. Berikut ini adalah infrastruktur software aplikasi SIMAK secara singkat :

1. Infrastruktur *software*



Gambar 3. 3 Infrastruktur aplikasi SIMAK

Sumber : UPTTIK Universitas Siliwangi

Penjelasan gambar :

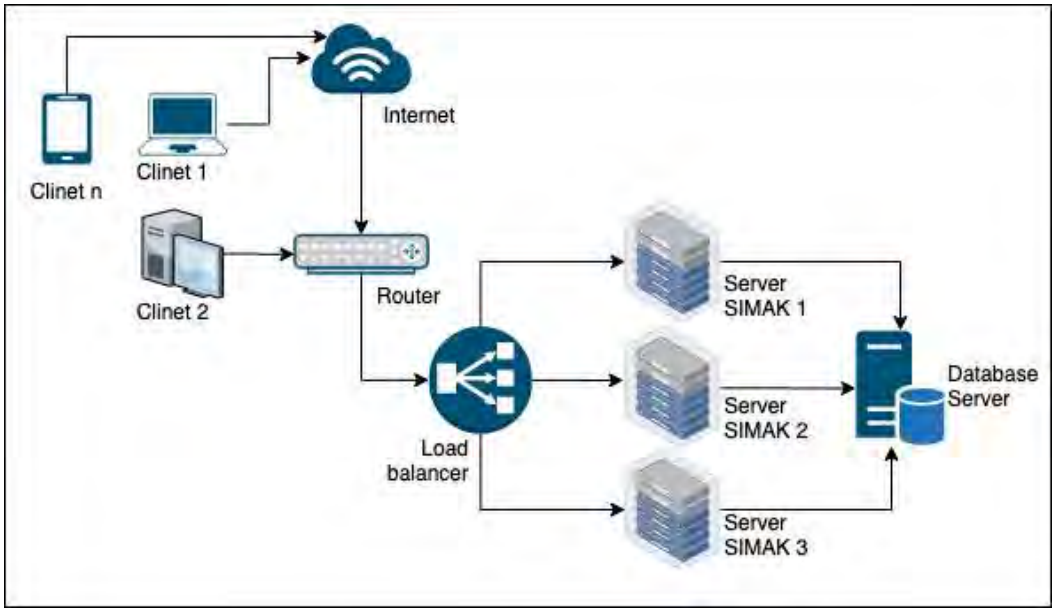
Secara singkat aplikasi SIMAK digambarkan pada gambar 3.3, dimana aplikasi SIMAK terdiri dari database aplikasi, dan aplikasi SIMAK itu sendiri. Tidak hanya database,

aplikasi SIMAK juga memiliki *chache database* yang berfungsi menopang kinerja aplikasi, *database* SIMAK menggunakan MariaDB sebagai manajemen pengolahan databasenya, sedangkah untuk bahsa pemrogaraman, aplikasi SIMAK menggunakan *(PHP : Hypertext Processor)* sebelum akhhirnya menjadi aplikasi dan dapat digunakan oleh *client.*

Server aplikasi SIMAK menggunakan sistem operasi CentOS, dan pengolahan manajemen database menggunakan MaraiaDB, sedangakan untuk versi PHP emnggunakan versi 5.4.

2. Infrastruktur *hardware*

Tidak hanya memerlukan software, aplikasi SIMAK juga memerlukan infrastruktur lain untuk dapat berjalan dengan baik dan dapat digunakan oleh *client,* infrastruktur tersebut yaitu infrastruktur *hardware,* aplikasi SIMAK memerlukan *server* fisik sebagai wadahnya, berikut adalah infrastruktur fisik aplikasi SIMAK secara singkat :



Gambar 3. 4 Infrastruktur fisik aplikasi SIMAK

Sumber : UPTTIK Universitas Siliwangi

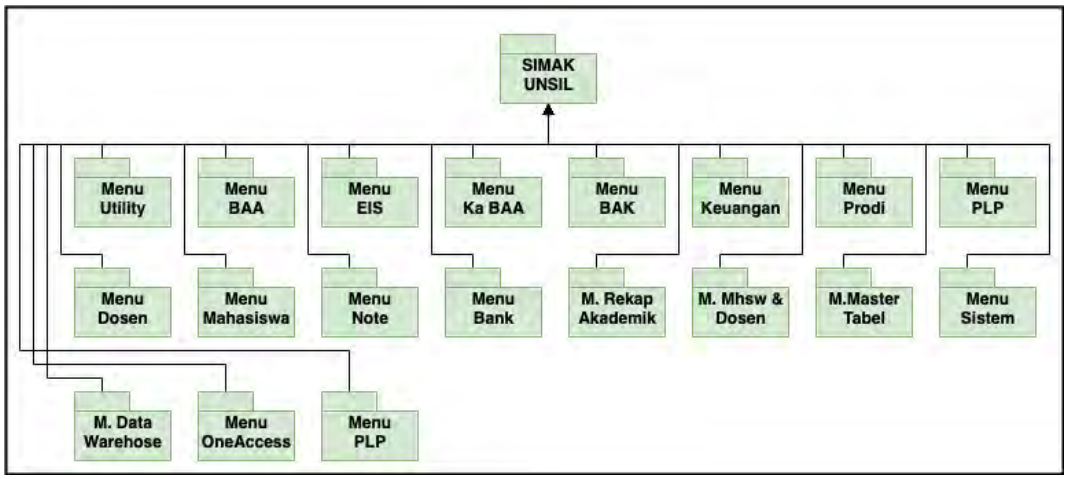
Seperti terliahat pada agambar 3.4 yaitu infrastruktur aplikasi SIMAK, terdapat 1 *server database* dab 3 *server* aplikasi, sebelum terhubung ke *router*, seluruh *request* dari

client dibagikan oleh *load balancer* ke 3 *server* aplikasi SIMAK, hal tersebut dilakukan supaya *load* atau kinerja aplikasi lebih ringan.

3.3.2. Desain Aplikasi SIMAK

Aplikasi SIMAK adalah aplikasi yang diperuntukan untuk mengatur segala jenis keperluan yang berhubungan dengan perkuliahan atau akademik. Aplikasi ini merupakan salah satu pelayanan bagi mahasiswa, dosen dan karyawan Universitas Siliwangi, aplikasi SIMAK dibuat untuk meningkatkan kinerja dan mempermudah urusan dalam hal akademik.

Aplikasi SIMAK berupa sistem yang berfungsi mengolah data kegiatan belajar mengajar seperti pengolahan data dosen, mahsiswa, nilai, matakuliah, jadwal mengajar, sampai dengan pembayaran atau registrasi semester mahasiswa, semua data tersebut diolah dan tersimpan pada aplikasi SIMAK yang dikelola oleh UPTTIK universitas Siliwangi. Secara singkat menu pada aplikasi SIMAK digambarkan pada Gambar 3.2 berikut :



Gambar 3. 5 Struktur menu aplikasi SIMAK

Sumber : UPTTIK Universitas Siliwangi

Berikut ini penjelasan Gambar 3.2 :

1. Menu *Utility*

   Pada menu ini terdapat beberapa fungsi, diantaranya yaitu : *Export* Data ke PDDIKTI, Rekap Data Dosen, Rekap Dosen Pembimbing, Rekap Perkembangan Mahasiswa dan Rekap Perkembangan Universitas.

2. Menu BAA

   Pada menu ini sebagian pengaturan dan fungsi akademik diatur, pada menu ini terdapat fungsi untuk pembagian kelas, menu untuk memindahkan mahasiswa dari satu prodi ke prodi yang lain, transkrip per semester, setak kartu hasil studi (KHS), transkrip nilai sementara, transkrip nilai akhir, administrasi wisuda, alumni, cetak ijazah, arsip penerbitan ijazah, dan cetak kartu mahasiswa. Menu BAA di kelola oleh admin Biro Administrasi Akademik.

3. Menu EIS

   Menu ini adalah menu yang dieperuntukan bagi pimpinan, menu EIS *(Enterprise Information System)* menyediakan rangkuman berbagai data hterkait perkembangan Universitas seperti, statistik perkembangan jumlah lulusan, statistik perkembangan peminat (calon mahasiswa baru) setiap tahun, jumlah program studi sampai dengan jumlah mahasiswa aktif Universitas Siliwangi.

4. Menu Ka. BAA

   Fungsi dari menu ini adalah pembukaan tahun akademik, menu ini dapat dikelola atau digunakan oleh Kepala Biro Akademik.

5. Menu BAK

   Pada menu ini terdapat fungsi untuk rekap beasiswa, cetak sertifikat Orientasi Mahasiswa Baru (OMBUS), rekap OMBUS, dan cetak sertifikat Pendidikan Pendahuluan Bela Negara (PPBN). Menu ini dipegang atau dioperasikan oleh staf dibagian akademik.

6. Menu Keuangan

Pada menu ini terdapat menu set tahun akademik keuangan, her registrasi dan pembayaran, pembayaran via bank, registrasi dan pembayaran transitoris, transitoris bank, honor dosen wali, sejarah pembayaran mahasiswa, honorarium pembayaran kelebihan mengajar, laporan keuangan, lapotran keuangan bank, laporan keuangan per fakultas samapai rekap penerimaan keuangan.

7. Menu Prodi

Menu prodi adalah menu yang dapat diakses oeleh ketua dan sekretaris program studi, pada menu ini terdapat menu set dosen wali, penjadwalan kuliah, presensi dosen dan mahasiswa, presentase nilai, penjadwalan ujian tengah semester, penjadwalan ujian akhir semester, komprehensif, manajemen kerja praktek, manajemen tugas akhir, konversi mahasiswa pindahan, Konversi pindah kurikulum lama , rekap jutrnal, konsentrasi program studi, pencarian judul skripsi, dan cetak kartu ujian.

8. Menu PLP

Menu ini diperuntukan bagi fakultas keguruan, padan menu ini terdpat menu tahun Praktek Kerja Lapanagan (PLP), daftar PLP, penempatan, rekap PLP, rekap peserta, penilaian, sampai dengan cetak sertifikat PLP.

9. Menu Dosen

Menu ini dapat diakses oleh ketua dan sekretaris program studi, pada menu ini terdapat fungsi atau sub menu jadwal mengajar, penilaian, dosen wali, walidasi Kartu Rencana Studi (KRS), rekap validasi dosen wali, ubah password dosen, sampai dengan SKPI.

10. Menu Mahasiswa

Pada menu ini terdapat fungsi cari amahasiswa, kartu rencana studi (KRS), nilai semester, sejarah nilai, ubah password mahasiswa, daftar wisuda, liahat transkrip, nonaktifkan matakuliah, daftar kuliah kerja nyata (KKN) dan validasi biaya uang kuliah tunggal (UKT).

11. Menu Bank

Pada menu ini terdapat fungsi untuk melihat data keuangan yang berhubungan dengan transitoris via bank, admin dapat mengambil dan mentransfer data yang berhubungan keuangan seperti laporan keuangan yang dibayarkan via bank oleh mahasiswa.

12. Menu Rekap Akademik

Pada menu ini terdapat fungsi untuk melihat rekap jurnal, melihat rekap nilai kosong, rekap nilai D, rekap target uang kuliah tunggal (UKT), rekap kegiatan mahasiswa, rekap yudisium, rekap yudisium perangkatan, rekap matakuliah, rekap indeks prestasi komulatif (IPK), rekap validasi kartu wrencana studi (KRS), rekap indeks prestasi komulatif (IPK) lulusan, rekap wisuda, dan rekap lulusan pertahun.

13. Menu Rekap Mahasiswa dan Dosen

Menu ini menyediakan fungsi mekap jumlah mahasiswa, rekap jumlah status mahasiswa, rekap status mahasiswa, portal mahasiswa, rekap dosen wali, dan rekap nisbah dosen.

14. Menu Master Tabel

Menu ini dapat di kelola atau dapat diakses oleh super admin yang berada di *level* rektorat, pada menu ini terdapat fungsi pejabat, fakultas, program studi, kampus, ruangan, dosen, mahasiawa, master baiaya dan potongan, master baiaya dan transitoris, matakuliah, koreksi nilai mahasiswa, dan status mahasiswa.

15. Menu Sistem

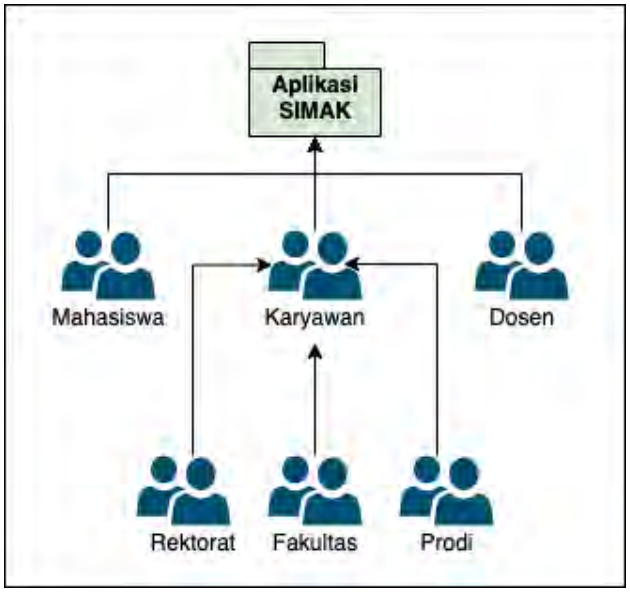
Menu ini adalah menu master yang dapat di kelola oleh admin yang berada di UPTTIK, pada menu ini terdapat submenu admin modul yaitu menu untuk menentuka seseorang menjadi salah satu *level* admin, admin user, dan alur diagram sistem.

16. Menu OneAccess

Menu ini adalah menu yang berfungsi untuk pengaturan akses jaringan yang dapat di gunakan untuk mahasiswa, pada menu ini admin dapat mendaftarkan pengguna baik dosen, mahasiswa sampai dengan karyawn untuk dapat mempunyai akun internet.

3.3.3. Pengguna Aplikasi SIMAK

Aplikasi SIMAK dapat di gunakan oleh beberapa *level* akses, yaitu dosen, karyawan dan mahasiswa. Sebagai mana dapat dilihat pada gambar berikut :



Gambar 3. 6 Pengguna aplikasi SIMAK
Sumber : UPTTIK Universitas Siliwangi

Penjelasan Gambar 3.3 adalah sebagai berikut :

Pengguna aplikasi SIMAK dibagi menjadi tiga kelompok utama yaitu :

1. Mahasiswa

Mahasiswa adalah pengguna utama aplikasi SIMAK, mahasiswa dapat mengakses data seperti data pribadi, data sejarah nilai, kontrak matakuliah, dan melakukan validasi pembayaran atau her-registrasi. Selain itu mahasiswa juga dapat mendaftar kerja praktek dan tugas akhir pada akun masing – masing.

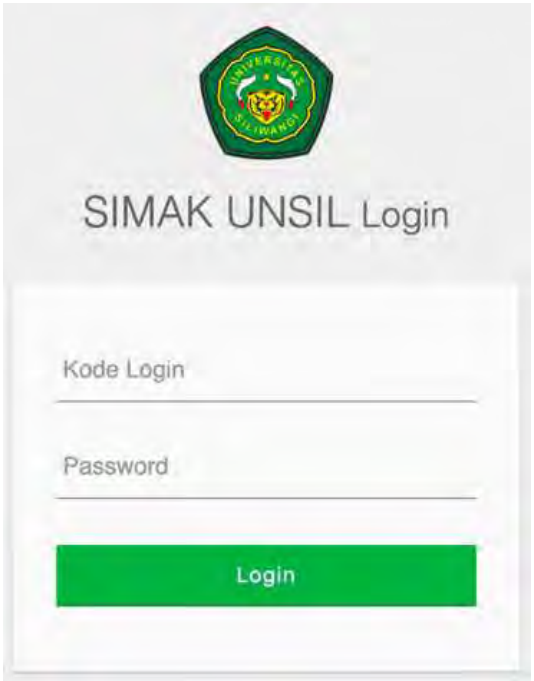
2. Karyawan

Karyawan pengguna aplikasi SIMAK dibagi menjadi tiga kelompok utama, yaitu pengguna yang berada pada *level* rektorat, fakultas dan jurusan atau program studi. Pada *level* rektorat terdapat pengguna yang berhak mengurusi masalah akademik, keuangan, dan kemahasiswaan, sama halnya dengan *level* rektorat, pada *level* fakultas dan program studi juga terdapat admin yang bertugas pada bidang akademik, mahasiswa dan keuangan namun dengan hak akses yang berbeda.

3. Dosen

Kewenangan dosen pada aplikasi SIMAK yaitu terkait dengan kemahasiswaan, seperti validasi kontrak matakuliah, input nilai mahasiswa, serta validasi pengajuan judul kerja praktek dan tugas akhir.

Ketiga kelompok *level* diatas memiliki hak akses yang berbeda sesuai dengan tugas dan fungsi masing – masing. Hak akses tersebut di buat dan di tentukan oleh administrator utama yang berada pada unit UPTTIK Universitas Siliwangi. Berikut ini adalah tampilan login aplikasi SIMAK :



Gambar 3. 7 Tampilan login aplikasi SIMAK

Semua akses baik dosen, mahasiswa, dan karyawan login pada halaman yang sama dengan menggunakan *username* dan *password* yang berbeda.

3.3.4. Masalah yang sering muncul

Selain dari rumusan masalah yang sudah disebutkan pada bab sebelumnya, terdapat beberapa masalah yang sering muncul terakait dengan cakuapan klausul pada penelitian ini. Masalah yang muncul seringkali menghambat bahkan merugikan organisasi baik kerugian waktu ataupun hilangnya kepercayaan pengguna terhadap aplikasi SIMAK.

Perkembangan kebutuhan mengharuskan UPTTIK merubah, menyesuaiakan bahkan menamabah menu atau modul pada aplikasi SIMAK, pada prakteknya UPTTIK terkadang tidak menerapkan prosedur standar dalam pengembangan SIMAK, hal ini memicu munculnya beberapa isu atau masalah yang berhubungan dengan keamanan informasi khusunya pada aplikasi SIMAK.

Berikut ini adalah beberapa masalah yang sering kali muncul pada aplikasi SIMAK :

1. Terkait dengan domain 5 (kebijakan keamanan informasi)

   Belum tersedianya peraturan terkait keamanan informasi pada aplikasi SIMAK, menyebabkan sering terjadinya penyalahgunaan informasi seperti penyalahgunaan *username* dan *password* aplikasi SIMAK, masih banyak pengguna aplikasi SIMAK yang belum menerapkan standar keamanan dalam menjaga kerahasiaan data pada aplikasi SIMAK, seperti menggunakan *password* yang tidak sesuai dengan standar keamanan.

2. Terkait dengan domain 6 (keamanan informasi organisasi)

   Belum diaturnya terkait keamanan informasi organisasi menyebabkan sering terjadinya kebocoran data yang dikelola oleh UPTTIK pada aplikasi SIMAK, seperti *password* aplikasi SIMAK, *password* jaringan, dan data – data lain yang bersifat rahasia. Selain itu juga terdapat permasalahan seperti belum adanya kebijakan

secara tertulis terkait kerja jarak jauh *(teleworking)*, juga belum tersedianya penilaian keamanan informasi terkait proyek yang dikerjakan.

3. Terkait dengan domain 9 (kontrol akses)

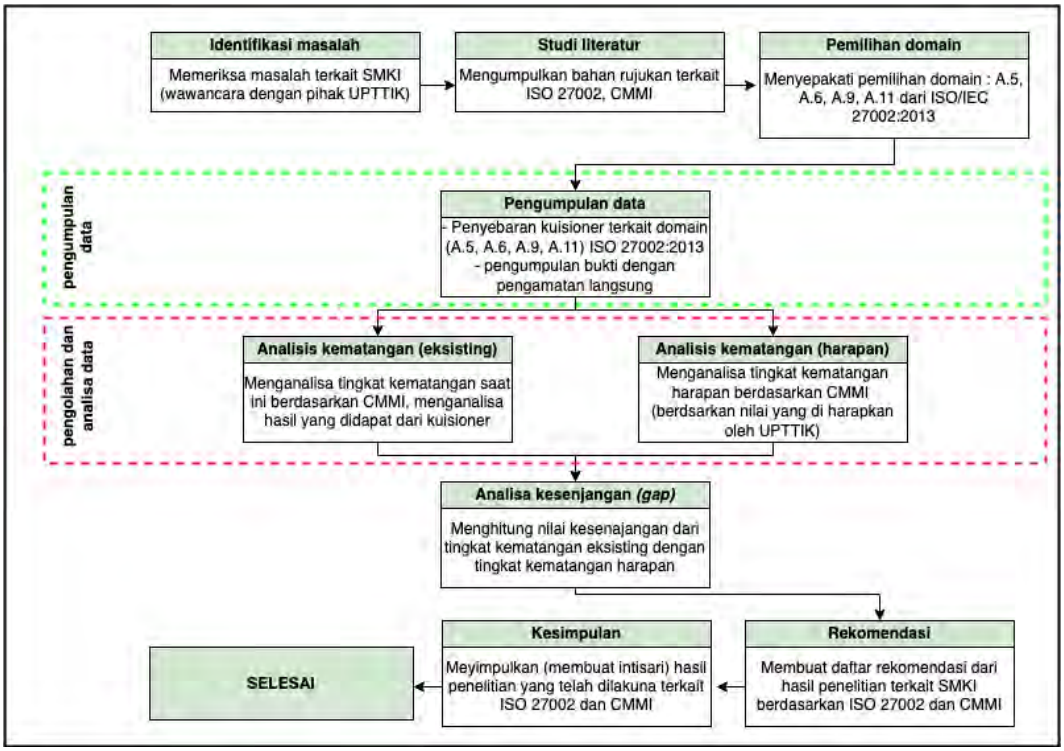
   Belum tersedianya peraturan yang mengatur tentang kontrol akses terkait menu atau modul yang berada pada aplikasi SIMAK menyebabkan sering terjadi ketidak jelasan terkait pengguna menu atau modul aplikasi. Selain itu juga pengelolaan hak akses administrator yang belum jelas juga menyebabkan tumpang tindihnya pengelolaan atas kewenangan merubah suatu data. Belum ada kebijakan yang mengatur terkait peninjauan dan penghapusan akases yang sudah tidak berlaku dapat memicu adanya akses illegal.

4. Terkait dengan domain 11 (keamanan fisik dan lingkungan)

   Tidak ada kebijakan pembatasan akses terhadap ruangan IT, menyebabkan sering terganggunaya *programmer* aplikasi SIMAK dalam pengembangan aplikasi. Ruangan sever yang tidak sesuai standar berisiko menimbulkan gangguan keamanan terhadap perangkat *server* aplikasi SIMAK.

3.4. Tahapan Penelitian

Proses penelitian yang akan dilakukan oleh penulis adalah dengan menganalisis aplikasi SIMAK dari awal sampai dengan akhir atau didapatnya suatu hasil analisis. Tahapan penelitian dapat dilihat pada gambar 3.2 berikut :



Gambar 3. 8 Tahapan Penelitian

Sumber : Penelitian 2020

Secara singkat pada gambar dapat dilihat bahwa proses penelitian dibagi menjadi dua kelompok, yang pertama adalah pengumpualan data, yang selanjutnya adalah pengolahan data dan menganalisa data.

3.4.1. Identifikasi masalah

Tahap ini merupakan tahap pertama dari penelitian, pada tahap ini melakukan identifikasi masalah di UPTTIK, yaitu dengan melakukan wawancara dengan pihak UPTTIK terkait masalah SMKI terutama menyangkut masalh aplikasi SIMAK, selain itu juga melakukan pengamatan langsung dilapangan terhadap penerapan aplikasi SIMAK yang dikelola oleh UPTTIK Universitas Siliwangi, pengamatan dilakukan terkait dengan domain yang sudah disepakati dalam penelitian.

Terkait dengan domain 5 yaitu kebijakan keamanan informasi, pengamatan dilakukan dengan melihat apakah semua kegiatan yang dilakukan terkait pengelolaan

aplikasi SIMAK sudah berdasarkan kebijakan keamanan informasi yang tersedia atau dibuat oleh organisasi.

Terkait dengan domain 6 yaitu keamanan informasi organisasi, pengamatan dilakukan yaitu dengan mengamati apakah pengelolaan aplikasi SIMAK sudah sesuai standar pada domain 6, domain 6 salah satu isinya tentang kebijakan kerja jarak jauh atau *teleworking*.

Terkait domain 9 yaitu kontrol akses, salah satu isinya terkait kontrol terahdap aplikasi, pada penelitian ini adala aplikasi SIMAK, juga termasuk disalamnya adalah pengelolaan kata sandi atau password. Penulis mengamati bagaimana pengelolaan password sampai ke tingkat pengguna, apakah UPTTIK sebagai pengelola aplikasi SIMAK sudah melakukan pengamanan password sampai ke tingkat pengguna, misalnya dengan melakukan penyuluhan terkait pentingnya mengelola password.

Terakait domain 11 yaitu keamanan fisik dan lingkungan, salah satu isi dari domain ini adalah terkait masalah perawatan dan perlindungan kabel jaringan atau kabel listrik yang digunakan untuk menjalankan aplikasi SIMAK, penulis mengamati apakah penempatan kabel listrik pada *server* aplikasi SIMAK sudah memenuhi standar atau belum, selain itu juga apakah terdapat kebijakan untuk selalu menerapkan standar *crear screen* dan *clear desk* dalam pengelolaan aplikasi SIMAK.

Selain melakukan pengamatan secara langsung, penulis juga melakukan wawancara terhadap unit terkait, dalam hal ini adalah kepala unit dan seluruh pegawai unit UPTTIK. Hasil dari wawacara tersebut berupa harapan dan gambaran terkait dengan aplikasi SIMAK terkait dengan kemajuan organisasi.

Pemeriksaan laporan dan standar operasional prosedur penggunaan terkait sistem informasi dan aplikasi SIMAK. Hasilnya adalah diperoleh tambahan data dan informasi untuk dapat diolah oleh penulis.

3.4.2. Studi literatur

Studi literatur dilakukan untuk dapat menjawab atas pertanyaan yang muncul dari hasil identifikasi masalah, studi literatur yaitu dengan mencari sumber dari berbagai lieratur yang terkait dengan penelitian yang dilakukan oleh penulis. Literatur yang digunakan mencakup jurnal terkait keamanan informasi, standar yang digunakan yaitu ISO 27000 *series*, juga jurnal terkait dengan penelitian yang telah dilakukan sebelumnya oleh penulis lain. Hasil dari studi literatur berupa kerangka berfikir yang dijadikan acuan dalam proses penelitian yang akan dilakukan penulis.

3.4.3. Pemilihan domain

Langkah ini adalah pemilihan domain atau klausul dari IS0 27002:3013 yang akan dijadikan fokus penelitian oleh penulis, pemilihan domain berdasarkan dari hasil analisis pada unit terkait dan hasil diskusi dengan kepala atau pimpinan unit beserta staf UPTTIK Universitas Siliwangi.

3.4.4. Kuisioner

Selanjutnya adalah melakuakan pengumpulan data dengan cara membagikan kuisioner kepada seluruh anggota unit. Kuisioner yang di susun adalah berdasarkan dari domain yang dipilih pada tahap sebelumnya. Seluruh anggota unit mengisi kuisioner untuk selanjutnya hasilnya diolah oleh penulis.

3.4.5. Analisis Kematangan existing dan harapan

Tahap ini penulis melakukan perbandingan kepada standar penerapan atau yang diterapkan terkait pengelolaan aplikasi SIMAK yang di kelola oleh UPTTIK, standar harapan yang di jadikan acuan adalah penggunaan standar ISO 27002 yaitu domain 5 (keabijakan keamanan informasi), domain 6 (keamanan informasi organisasi), domain 7 (keamanan sumberdaya manusia, domain 9 (kontrol akses), dan domain 11 (keamanan fisik dan lingkungan).

Tahapan ini dilakukan untuk melakukan analisa adari data yang telah didapatakan dari langkah pengumpulan data di UPTTIK Universitas Siliwangi berdasarkan *Capability Maturity Model Integration* (CMMI). Hasilnya adalah berupa niali yang dihasilkan dari penilaian tingkat kematangan terkait dengan kalusul yang telah dipilih dan disepakati sebelumnya.

Pada penelitian ini penulis meneyebarkan kuisioner dan melakukan wawancara kepada pihak terkait guna menegetahui proses aplikasi SIMAK terkait cakupan domain yang sepakati.

3.4.6. Analisis Kesenjangan

Dalam bisnis, analisis gap adalah suatu analisis yang dilakukan untuk menentukan langkah – langkah yang harus diambil untuk dapat berpindah dari kondisi saat ini ke kondisi harapan. Pada penelitian ini analisis kesenjangan digunakan untuk menentukan langkah yang harus di ambil selanjutnya oleh organisasi guna untuk mencapai target capaian terkait dengan keamanan informasi khusunya terkait dengan domain cakupan penelitan yang telah disepakati. Kondisi harapan pada penelitian ini yaitu kondisi yang diharapkan oleh organisasi yang berdasarkan atas standar ISO/IEC 27002:2013.

3.4.7. Rekomendasi

Setelah melakukan *gap* analisis atau melakukan analisa kesenjangan, langkah selanjutnya yang dilakukan penulis adalah menentukan atau membuat daftar rekomendasi untuk dapat dilakukan oleh UPTTIK untuk melakukan perbaikan diamasa yang akan datang.

Dalam melakukan penentuan rekomendasi, rekomendasi didapatkan dari hasil data dan penelitian yang telah dilakukan yaitu terkait dengan data yang ada pada UPTTIK, seperti data prosedur standar opersional unit, kebijakan, dan portofolio terkait dengan penelitian yang dilakukan. Selain itu juga dilakukan observasi lapangan, wawancara terhadap penanggungjawab aplikasi SIMAK. Seluruh langkah dan kegiatan tersebut menghasilkan bukti yang dapat dijadikan untuk dapat menghasilkan rekomendasi.

3.4.8. Penarikan Kesimpulan

Penulis menyimpulkan hasil dari penelitian yang dilakukan di UPTTIK, kesimpulan ini berupa rangkuman atau intisari dari penelitian yang telah dilakukan.

Penarikan kesimpulan merupakan langkah akhir dari proses penelitian, dimana penulis dengan hasil penelitian yang telah dilakukannya, yaitu dari bukti dan data – data yang dikumpulkan harus dapat menarik kesimpulan.

Kesimpulan tersebut dihasilkan berdasarkan hasil analisis *gap* dan rekomendasi. Kesimpulan tersebut berupa jawaban akhir yang dihasilkan dari penelitian yang telah dilakukan penulis. Kesimpulan tersebut dapat dijadikan acuan bagi UPTTIK dalam melakukan perbaikan dan penyempurnaan keamanan informasi pada sistem atau apalikasi yang dikelolanya.

3.5. Pengumpulan Data

Langakah pengumpulan data yang dilakukan oleh penulis dibagi menjadi dua kelompok, yaitu data primer dan data sekunder yang merupakan data pendukung dalam penelitian ini, data primer adalah data utama yang diperoleh dari observasi, wawancara dan survei.

3.5.1. Observasi

Langkah observasi adalah langkah pengumpulan data yang dilakukan oleh penulis yaitu dengan cara pengamatan secara langsung dilapangan, pengamatan yang dilakukan meliputi melihat secara langsung penerapan standar keamanan yang dilakukan pada aplikasi SIMAK yang dilakukan oeleh pengelola aplikasi yaitu UPTTIK Universitas Siliwangi.

3.5.2. Wawancara

Langkah ini dilakukan denga melakukan wawancara langsung kepada narasumber yaitu pegawai UPTTIK sebagai orang yang secara langsung bertanggungjawab mengelola aplikasi SIMAK.

3.5.3. Survei

Langkah survei adalah langkah dimana penulis memberikan pertanyaan berupa kuisioner kepada karyawan UPTTIK Universitas Siliwangi, kuisioner yang dibuat meliputi hal – hal yang mencakup penelitian yang dilakukan oleh penulis yanitu terkait domain yang telah disepakati terlebih dahulu dengan pimpinan unit.

Domain atau klausul yang disepakati tersebut dapat dilihat pada Tabel 3.1

Tabel 3. 1 Domain yang disepakati

Domain	Penjelasan
A.5	Terkait kebijakan keamanan informasi
A.6	Terkait keamanan informasi organisasi
A.9	Terkait Kontrol Akses
A.11	Terkait Keamanan Fisik dan Lingkungan

Sumber : ISO 27002:2013

Tabel 3. 2 Rincian domain yang disepakati ISO/IEC 27002:2013

A.5	Kebijakan Keamanan Informasi
A.5.1	Arahan manajemen untuk keamanan informasi
A.5.1.1	Kebijakan untuk keamanan informasi
A.5.1.2	*Review* kebijakan untuk keamanan informasi
A.6	Organisasi keamanan informasi
A.6.1	Organisasi Internal
A.6.1.1	Peran dan tanggung jawab keamanan informasi
A.6.1.2	Pemisahan tugas
A.6.1.3	Kontak dengan pihak berwenang
A.6.1.4	Kontak dengan kelompok minat khusus
A.6.1.5	Keamanan informasi dalam manajemen proyek
A.6.2	Perangkat Seluler dan *Teleworking*
A.6.2.1	Kebijakan perangkat seluler
A.6.2.2	*Teleworking*
A.9	Kontrrol Akses
A.9.1	Persyaratan bisnis untuk kontrol akses
A.9.1.1	Kebijakan Kontrol Akses
A.9.1.2	Akses ke jaringan dan layanan jaringan
A.9.2	Manajemen akses pengguna
A.9.2.1	Pendaftaran pengguna dan pencabutan pendaftaran

Tabel 3. 3 Rincian domain yang disepakati ISO/IEC 27002:2013 (Lanjutan)

A.9.2.2	Penyediaan akses pengguna
A.9.2.3	Pengelolaan hak akses istimewa
A.9.2.4	Pengelolaan informasi otentikasi rahasia pengguna
A.9.2.5	*Review* hak akses pengguna
A.9.2.6	Penghapusan atau penyesuaian hak akses
A.9.3	Tanggung jawab pengguna
A.9.3.1	Penggunaan informasi otentikasi rahasia
A.9.4	Kontrol akses sistem dan aplikasi
A.9.4.1	Pembatasan akses informasi
A.9.4.2	Amankan prosedur log-on
A.9.4.3	Sistem manajemen kata sandi
A.9.4.4	Penggunaan program utilitas dengan hak istimewa
A.9.4.5	Kontrol akses ke kode sumber program
A.11	Keamanan fisik dan lingkungan
A.11.1	Area aman
A.11.1.1	Perimeter keamanan fisik
A.11.1.2	Kontrol entri fisik
A.11.1.3	Mengamankan kantor, kamar, dan fasilitas
A.11.2	Peralatan
A.11.2.1	Penempatan dan perlindungan peralatan
A.11.2.2	Utilitas pendukung
A.11.2.3	Keamanan kabel
A.11.2.4	Perawatan peralatan
A.11.2.5	Penghapusan aset
A.11.2.6	Keamanan peralatan dan aset di luar lokasi
A.11.2.7	Pembuangan yang aman atau penggunaan kembali peralatan
A.11.2.8	Peralatan pengguna tanpa pengawasan
A.11.2.9	Kebijakan *Clear desk and clear screen*

Sumber : ISO/IEC 27002:2013

Kuisioner yang dibaut dan diberikan kepada responden meliputi 5 domain yang teradapat pada ISO 27002 yaitu mengenai domain 5 (keabijakan keamanan informasi), domain 6 (keamanan informasi organisasi), domain 9 (kontrol akses), dan domain 11 (keamanan fisik dan lingkungan).

Data kedua yang digunakan penulis dalam penelitian ini adalah data sekunder, merupakan data yang diperoleh dari hasil studi pustaka, seperti jurnal, buku dan website.

3.6. Alasan pemilihan domain

Ada beberapa alasan mendasar mengenai pemilihan domain pada penelitian ini, salah satunya yaitu, pemilihan domain didasarkan pada hasil kesepakatan antara penulis dengan kepala UPTTIK. Sedangkan alasan lain yang terkait dengan domain yang dipilih

adalah kerap muncul permasalahan dan sebagai langkah antisipasi munculnya permasalahan baru yang mungkin muncul dikemudian hari.

BAB IV

HASIL DAN PEMBAHASAN

4.1. Penetapan Domain

Langkah observasi yang telah dilakukan sebelumnya menghasilkan penertapan ruang lingkup analisis, ruang lingkup tersebut terkait dengan keamanan informasi juga standar yang dipakai yaitu ISO 27002:2013. Selain itu juga, dari hasil observasi dan wawancara terhadap pihak terkait yaitu UPTTIK Universitas Siliwangi maka di sepakati terkait domain yang akan dipakai dalam penelitian ini.

Dalam penelitian ini domain yang disepakati dengan UPTTIK Universitas Siliwangi sebagai penanggungjawab aplikasi SIMAK adalah empat domain atau klausul, domain – domain tersebut adalah domain A.5 tentang kebijakan keamanan informasi, domain A.6 tentang kebijakan keamanan organisasi, domain A.9 tentang kontrol akses dan yang terakhir adalah domain A.11 yaitu tentang keamanan fisik dan lingkungan.

Tabel yang berisi tentang domain yang disepakati dapat dilihat pada Table 3.3 pada BAB III.

Selain empat domain dari ISO 27002:2013 yang telah disepakati, terdapat juga domain yang tidak dipakai dari ISO/IEC 27002:2013. Domain tersebut adalah sebagai berikut :

Tabel 4. 1 Domain yang tidak diapakai

A.7	Keamanan sumber daya manusia
A.7.1	Sebelum bekerja
A.7.1.1	Penyaringan
A.7.1.2	Syarat dan ketentuan kerja
A.7.2	Selama bekerja
A.7.2.1	Tanggung jawab manajemen
A.7.2.2	Kesadaran keamanan informasi, pendidikan dan pelatihan
A.7.2.3	Proses disipliner
A.7.3	Pemutusan hubungan kerja dan perubahan pekerjaan
A.7.3.1	Pemutusan hubungan kerja atau perubahan tanggung jawab pekerjaan
A.8	Manajemen aset
A.8.1	Tanggung jawab atas aset
A.8.1.1	Inventaris aset
A.8.1.2	Kepemilikan aset
A.8.1.3	Penggunaan aset yang dapat diterima
A.8.1.4	Pengembalian aset
A.8.2	Klasifikasi informasi

Tabel 4. 2 Domain yang tidak diapakai (Lanjutan)

A.8.2.1	Klasifikasi informasi
A.8.2.2	Pelabelan informasi
A.8.2.3	Penanganan aset
A.8.3	Penanganan media
A.8.3.1	Pengelolaan media yang dapat dilepas
A.8.3.2	Pembuangan media
A.8.3.3	Transfer media fisik
A.10	Kriptografi
A.10.1	Kontrol kriptografi
A.10.1.1	Kebijakan tentang penggunaan kontrol kriptografi
A.10.1.2	Manajemen kunci
A.12	Keamanan operasi
A.12.1	Prosedur dan tanggung jawab operasional
A.12.1.1	Prosedur operasi yang terdokumentasi
A.12.1.2	Ubah manajemen
A.12.1.3	Manajemen kapasitas
A.12.1.4	Pemisahan lingkungan pengembangan, pengujian dan operasional
A.12.2	Perlindungan dari malware
A.12.2.1	Kontrol terhadap malware
A.12.3	Cadangan
A.12.3.1	Cadangan informasi
A.12.4	Logging dan pemantauan
A.12.4.1	Pencatatan acara
A.12.4.2	Perlindungan informasi log
A.12.4.3	Administrator dan log operator
A.12.4.4	Sinkronisasi jam
A.12.5	Pengendalian perangkat lunak operasional
A.12.5.1	Pemasangan perangkat lunak pada sistem operasional
A.12.6	Manajemen kerentanan teknis
A.12.6.1	Manajemen kerentanan teknis
A.12.6.2	Batasan penginstalan perangkat lunak
A.12.7	Pertimbangan audit sistem informasi
A.12.7.1	Pengendalian audit sistem informasi
A.13	Keamanan komunikasi
A.13.1	Manajemen keamanan jaringan
A.13.1.1	Kontrol jaringan
A.13.1.2	Keamanan layanan jaringan
A.13.1.3	Pemisahan dalam jaringan
A.13.2	Transfer informasi
A.13.2.1	Kebijakan dan prosedur transfer informasi
A.13.2.2	Kesepakatan tentang transfer informasi
A.13.2.3	Pesan elektronik
A.13.2.4	Perjanjian kerahasiaan atau kerahasiaan
A.14	Akuisisi, pengembangan dan pemeliharaan sistem
A.14.1	Persyaratan keamanan sistem informasi
A.14.1.1	Analisis dan spesifikasi persyaratan keamanan informasi
A.14.1.2	Mengamankan layanan aplikasi di jaringan publik
A.14.1.3	Melindungi transaksi layanan aplikasi
A.14.2	Keamanan dalam proses pengembangan dan dukungan
A.14.2.1	Kebijakan pembangunan yang aman
A.14.2.2	Prosedur kontrol perubahan sistem
A.14.2.3	Tinjauan teknis aplikasi setelah perubahan platform operasi

Tabel 4. 3 Domain yang tidak diapakai (Lanjutan)

A.14.2.4	Batasan perubahan paket perangkat lunak
A.14.2.5	Prinsip rekayasa sistem yang aman
A.14.2.6	Lingkungan pengembangan yang aman
A.14.2.7	Pengembangan outsourcing
A.14.2.8	Pengujian keamanan sistem
A.14.2.9	Pengujian penerimaan sistem
A.14.3	Uji data
A.14.3.1	Perlindungan data uji
A.15	Hubungan pemasok
A.15.1	Keamanan informasi dalam hubungan pemasok
A.15.1.1	Kebijakan keamanan informasi untuk hubungan pemasok
A.15.1.2	Mengatasi keamanan dalam perjanjian pemasok
A.15.1.3	Rantai pasokan teknologi informasi dan komunikasi
A.15.2	Manajemen pengiriman layanan pemasok
A.15.2.1	Pemantauan dan peninjauan layanan pemasok
A.15.2.2	Mengelola perubahan pada layanan pemasok
A.16	Manajemen insiden keamanan informasi
A.16.1	Manajemen insiden dan peningkatan keamanan informasi
A.16.1.1	Tanggung jawab dan prosedur
A.16.1.2	Melaporkan peristiwa keamanan informasi
A.16.1.3	Melaporkan kelemahan keamanan informasi
A.16.1.4	Penilaian dan keputusan tentang peristiwa keamanan informasi
A.16.1.5	Tanggap terhadap insiden keamanan informasi
A.16.1.6	Belajar dari insiden keamanan informasi
A.16.1.7	Pengumpulan bukti
A.17	Aspek keamanan informasi dari manajemen kelangsungan bisnis
A.17.1	Kontinuitas keamanan informasi
A.17.1.1	Perencanaan kontinuitas keamanan informasi
A.17.1.2	Menerapkan kontinuitas keamanan informasi
A.17.1.3	Verifikasi, tinjau dan evaluasi kontinuitas keamanan informasi
A.17.2	Redundansi
A.17.2.1	Ketersediaan fasilitas pengolahan informasi
A.18	Pemenuhan
A.18.1	Kepatuhan dengan persyaratan hukum dan kontrak
A.18.1.1	Identifikasi undang-undang yang berlaku dan persyaratan kontrak
A.18.1.2	Hak kekayaan intelektual
A.18.1.3	Perlindungan catatan
A.18.1.4	Privasi dan perlindungan informasi pengenal pribadi
A.18.1.5	Peraturan kontrol kriptografi
A.18.2	Tinjauan keamanan informasi
A.18.2.1	*Review* independen atas keamanan informasi
A.18.2.2	Kepatuhan terhadap kebijakan dan standar keamanan
A.18.2.3	Tinjauan kepatuhan teknis

Sumber : ISO 27002:2013

4.2. Penentuan *Working Plan*

Proses penelitian mengenai analisis sistem keamanan informasi yang bertempat di UPTTIK Universitas Siliwangi dilakukan secara bertahap dimulai dengan studi literatur

sampai dengan penyusunan laporan pemeriksaan, urutan kegiatan penelitain dituangkan dalam tabel *working plan* dan dapat dilihat pada tabel 4.4:

Tabel 4. 4 *Working Plan*

No	Nama Kegiatan	Bulan															
		September				Oktober				November				Desember			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1.	Melakukan studi literatur																
2.	Menentukan cakupan ruang lingkup penelitian																
3.	Mengumpulkan bukti																
4.	Melaksanakan pengujian terhadap kepatuhan																
5.	Menentukan *maturity level*																
6.	Menentukan hasil penelitan																
7.	Melakukan penyusunan terhadap hasil penelitian																

Penjelasan *working plan* penelitian adalah sebagai berikut :

1. Melakukan studi literatur

   Studi literatur dilakukan adari awal penelitian yaitu minggu pertama bulan September sampai dengan minggu ke 4 bulan Desember, studi literatur yaitu dengan mengumpulakan sumber – sumber terkait dengan penelitian seperti jurnal dan sumber lainnya.

2. Menentukan cakupan ruang lingkup penelitian

   Apada tahap ini penulis berkomunikasi dengan UPTTIK Universitas Siliwangi membahas tentang cakupan atau batasan penelitian yang akan dialakukan, kegiatan ini dilakukan pada minggu pertama bulan September samapai dengan minggu kedua bulan Oktober.

3. Mengumpulkan bukti

   Tahap ini dilakukan pengumpulan bukti terkait penelitian dianataranya adalah peninjauan struktur organisasi, peninjauan kenijakan dan prosedur terkait teknologi informasi organisasi, peninjauan standar terkait teknologi informasi,

peninjauan dokumentasi pengelolaan teknologi informasi dan proses wawancara dengan staf UPTTIK Universiatas Siliwangi.

4. Melaksanakan pengujian terhadap kepatuhan

   Tahap ini dilakukan pengolahan data yang dihasilakan dari tahap sebelumnya, data yang terkumpul di hitung untuk melakukan tahap selanjutnya. Kegiatan ini dilakukan pada minggu ke dua bulan Oktober sampai dengan minggu ke dua bulan November.

5. Menentukan *maturity level*

   Tahap menentukan *Maturity level* atau tingkat kematangan dilakukan pada minggu ke dua bulan Oktober samapai denagan minggu ke dua bulan November.

6. Menentukan hasil penelitan

   Kegiatan penentuan hasil penelitian dilakuakan pada minggu kedua bulan November sampai dengan minggu kedua bulan Desember, pada tahap ditentukan hasil uji penelitian yang telah dilakuakan.

7. Melakukan penyusunan terhadap hasil penelitian

   Tahap terakhir yaitu Menyusun hasil penelitian kedalah sebuah laporan, hasil tersebut berupa temuan – temuan yang didapat pada saat penelitian dilakukan. Tahap ini dilaksanakan pada minggu pertama bulan Desember sampai dengan minggu keempat bulan Desember.

4.3. Hasil Pengumpulan Data

Data – data yang di himpun atau di kumpulkan dapat berupa dokumen seperti foto, video atau dokumen lain yang terkait dengan penelitian, data tersebut dihasilkan saat pelaksanaan pemeriksaan yang dilakukan oleh peneliti.

Tabel 4.5 berisi hasil temuan dan bukti terkait domain lima yaitu tentang kebijakan keamanan.

Tabel 4. 5 Hasil temuan dan bukti

Domain	:	A.11	Keamanan fisik dan lingkungan
Kategori keamanan Utama	:	A.11.1	Area aman *(secure area)*
Kontrol Keamanan	:	A.11.1.1	Perimeter (pembatas) keamanan fisik

No.	Pernyataan	Hasil Pemeriksaan
1.	Ruang server SIMAK dilindungi keamanan fisik berupa (pembatas kaca, dinding beton, kunci sidik jari)	Ruang server SIMAK telah dikendalikan dengan cukup baik, diantaranya terdapat pembatas kaca, pembatas dinding beton, kunci sidik jari dua lapis.

4.4. Pemrosesan Data Kematangan

Bukti yang terkumpul dari hasil pemeriksaan dan pengumpulan barang bukti yang dilakukan oleh peneliti maka dihasilkan perhitungan untuk setiap kontrol.

Tingkat kematangan diperoleh dari hasil perhitungan kerangka kerja yang dapat dilihat pada Lampiran A.

Dari hasil perhitungan tingkat kematangan yang dilakukan peneliti terkait audit keamanan SIMAK adalah sebagai berikut :

1. Hasil tingkat kematangan Domain A.5 : Kebijakan keamanan informasi

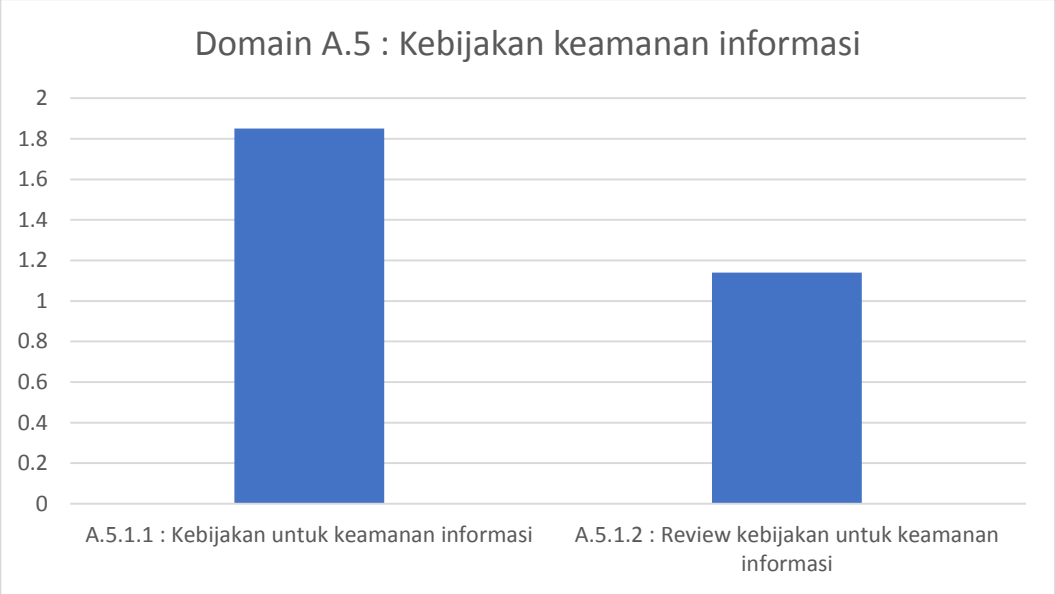
Proses perhitungan tingkat kematangan pada Domain A.5 yaitu tentang kebijakan keamanan informasi adalah 1,49 yang berarti initial, tidak ada kebijakan secara tertulis yang dikeluarkan oleh pimpinan dalam hal keamanan informasi aplikasi SIMAK atau tidak terdapat dokumentasi, kebijakan hanya bersifat lisan dari kepala UPTTIK kepada karayawan UPTTIK, informasi tidak merata kepada seluruh karyawan, tidak ada *guide line* terkait keamanan informasi, kebijakan keamanan informasi harus mencakup definisi keamanan informasi, penugasan dan tanggungjawab, proses menangani penyimpangan atau pelanggaran. Topik kebijakan keamanan informasi adalah terkait kontrol akses, klasifikasi informasi, keamanan fisik dan lingkungan dan lain-lain. Hasil perhitungan tingkat kematangan domain A.5 dapat dilihat pada Tabel 4.6.

Tabel 4. 6 Hasil perhitungan tingkat kematangan Domain A.5

Hasil perhitungan tingkat kematangan Domain A.5 dalam bentuk grafik adalah sebagai

Domain	Objektif kontrol	Kontrol keamanan	Tingkat kemampauan	Rata-rata objektif kontrol
A.5 : Kebijakan Keamanan Informasi	A.5.1 : Arahan manajemen untuk keamanan informasi	A.5.1.1 : Kebijakan untuk keamanan informasi	1,85	1,49
		A.5.1.2 : *Review* kebijakan untuk keamanan informasi	1,14	
Tingkat kematangan Domain A.5				1,49

berikut :



Gambar 4. 1 Grafik hasil perhitungan tingkat kematangan Domain A.5

2. Hasil tingkat kematangan Domain A.6 : Keamanan Informasi Oraganisasi

Proses perihitungan tingkat kematangan Domain A.6 yaitu tentang keamanan informasi organisasi adalah 1,52 atau berada pada *level repeatable*, dimana organisasi sudah berkomitmen untuk merencanakan proses standar. Banyak kontrol yang belum dilakukan terkait dengan keamanan informasi organisasi, diantaranya adalah asset dan proses keamanan informasi harus diidentifikasi dan ditetapkan, entitas yang bertanggungjawab terhadap setiap asset atau proses keamanan informasi harus ditetapkan serta tanggungjawabnya harus terinci dan didokumentasikan. Belum adanya

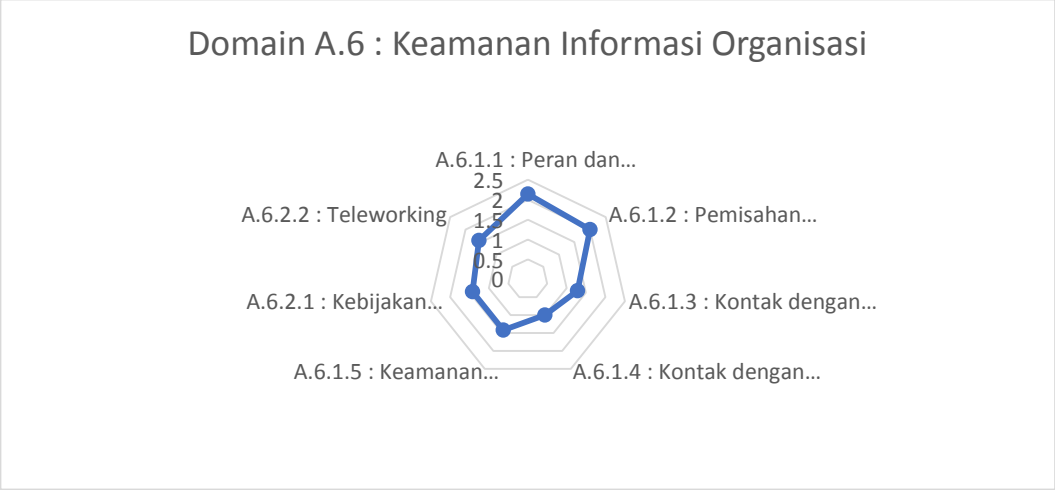
standar pengawasan terhadap keamanan pengembangan aplikasi SIMAK juga dapat memicu risiko keamanan yang dapat mengancam integritas data. Kebijakan terkait *teleworking* yang hanya bersifat lisan dan tidak ada panduan secara tertulis juga dapat menimbulkan risiko keamanan, misalnya terkait lingkunagan tempat *teleworking*, atau ancaman eksternal terhadap *asset* yang digunakan untuk melakukan *teleworking*.

Berikut ini adalah tabel 4.7 hasil perhitungan tingkat kematangan Domain A.6 yaitu tentang keamanan informasi organisasi :

Tabel 4. 7 Hasil perhitungan tingkat kematangan Domain A.6

Domain	Objektif kontrol	Kontrol keamanan	Tingkat kemampauan	Rata-rata objektif kontrol
A.6 : Keamanan Informasi Organisasi	A.6.1 : Internal Organisasi	A.6.1.1 : Peran dan tanggung jawab keamanan informasi	2,14	1,56
		A.6.1.2 : Pemisahan tugas	2	
		A.6.1.3 : Kontak dengan pihak berwenang	1,28	
		A.6.1.4 : Kontak dengan kelompok minat khusus	1	
		A.6.1.5 : Keamanan informasi dalam manajemen proyek	1,42	
	A.6.2 : Perangkat Seluler dan *Teleworking*	A.6.2.1 : Kebijakan perangkat seluler	1,42	1,49
		A.6.2.2 : *Teleworking*	1,57	
Tingkat kematangan Domain A.6 Keamanan informasi organisasi				1,52

Hasil perhitungan tingkat kematangan Domain A.6 dalam bentuk grafik adalah sebagai berikut :



Gambar 4. 2 Grafik hasil perhitungan tingkat kematangan Domain A.6

3. Hasil tingkat kematangan Domain A.9 : Kontrol akses

Perhitungan tingkat kematangan pada Domain A.9 terkait kontrol akses medapatkan nilai 1,32 atau berada pada level *initial,* dimana proses standar telah dilakukan namun masih bersifat informal dan tidak mengacu pada suatu standar tertentu. Pada prakteknya banyak kontrol keamanan yang dilakukan namun belum mengikuti suatu standar. Pendaftaran pengguna (pegawai atau dosen) sudah dilakukan berdasarkan surat keputusan yang dikeluarkan dari pihak kepegawaian, kemudian diterjemahkan atau dibuatkan hak akses berdasarkan jabatan yang dimiliki oleh pengguna.

Kontrol akses pada server aplikasi SIMAK dilakukan menggunakan akses VPN *(Virtual Private Network)* dan didaftarkan langsung oleh admin jaringan, proses pendaftan dilakukan berdasarkan intruksi lisan dari pimpinan UPTTIK dan belum secara tertulis. Kontrol lain yang juga masih dilakukan secara informal seperti manajemen ID pengguna dan lain sebagainya.

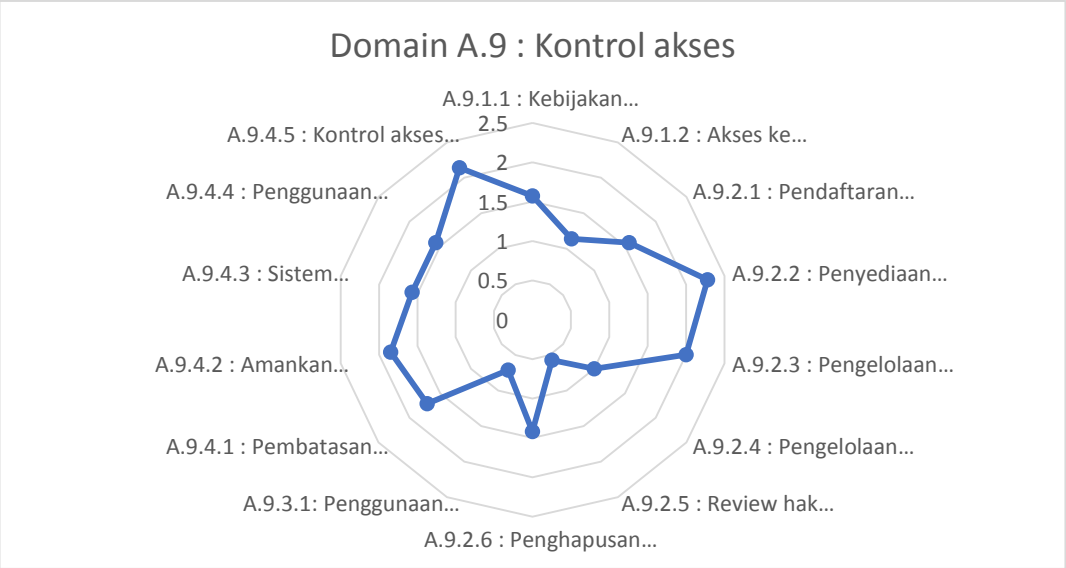
Terkait manajemen hak akses istimewa atau akses *root* terhadap sistem operasi, database dan *source code* aplikasi SIMAK dilakukan oleh satu orang pegawai yang ahli.

Berikut ini adalah tabel 4.8 hasil perhitungan tingkat kematangan Domain A.9 terntang Kontrol akses :

Tabel 4. 8 Hasil perhitungan tingkat kematangan Domain A.9

Domain	Objektif kontrol	Kontrol keamanan	Tingkat kemampauan	Rata-rata objektif kontrol
A.9 : Kontrol akses	A.9.1 : Persyaratan bisnis untuk kontrol akses	A.9.1.1 : Kebijakan kontrol akses	1,57	1,35
		A.9.1.2 : Akses ke jaringan dan layanan jaringan	1,14	
	A.9.2 : Manajemen akses pengguna	A.9.2.1 : Pendaftaran dan pencabutan akses pengguna	1,57	1,47
		A.9.2.2 : Penyediaan akses pengguna	2,28	
		A.9.2.3 : Pengelolaan hak akses istimewa	2	
		A.9.2.4 : Pengelolaan informasi otentikasi rahasia pengguna	1	
		A.9.2.5 : *Review* hak akses pengguna	0,57	
		A.9.2.6 : Penghapusan atau penyesuaian hak akses	1,42	
	A.9.3 : Tanggung jawab pengguna	A.9.3.1: Penggunaan informasi otentikasi rahasia	0,71	0,71
	A.9.4 : Kontrol akses sistem dan aplikasi	A.9.4.1 : Pembatasan akses informasi	1,71	1,76
		A.9.4.2 : Amankan prosedur log-on	1,85	
		A.9.4.3 : Sistem manajemen kata sandi	1,57	
		A.9.4.4 : Penggunaan program utilitas dengan hak istimewa	1,57	
		A.9.4.5 : Kontrol akses ke kode sumber program	2,14	
Tingkat kematangan Domain A.9 Kotrol akses				1,32

Hasil perhitungan tingkat kematangan dalam bentuk grafik adalah sebagai berikut :



Gambar 4. 3 Grafik hasil perhitungan tingkat kematangan Domain A.9

4. Hasil tingkat kematangan Domain A.11 : Keamanan fisik dan lingkungan

Perhitungan tingkat kematangan Domain A.11 atau terkait Keamanan fisik dan lingkungan mendapatkan hasil dengan nilain 1,97 atau berada pada level 2 *(repeatable)* proses ini diartikan dimana organisasi sudah berkomitmen untuk merenca. nakan proses standar. Ada beberapa kontrol yang perlu diperhatikan atau diperbbaiki diantaranya adalah adanya celah dinding kaca yang menyekat antara ruang *server* yang berbatasan langsung dengan ruang rapat utama dimana ruang tersebut secara bebas dapat diakses oleh banyak orang. Sedangkan pada kontrol entri fisik ruangan *server* aplikasi SIMAK sudah dilindungi oleh 2 lapis pengamanan pintu yang dikunci oleh kunci sidik jari, kunci tersebut hanya bisa dibuka oleh orang yang telah terotorisasi atau telah didaftrakan aksesnya. Pada kontrol keamanan 11.1.4 yaitu tentang terlindung dari ancaman eksternal dan lingkungan ruang server berada dilantai 2 atau dengan katalain dapat terbebas dari bencana banjir. Ruangan server sendiri pada perancangannya belum dirancang sebagai ruangan server, namun hanya sebagai ruangan kantor biasa. Terdapat *secure area* dimana area stersebut berada ditengah ruangan antara ruangan karyawan luar dan ruangan *server*, pada area ini sama

hanya pada ruangan server tamu atau orang yang tidak berkepentingan dilarang memotret dan tamu diwajibakan memakai ID card atau tanda pengenal untuk dapat diizinkan masuk.

Terkait dengan kontrol objektif 11.2 atau tentang peralatan, server aplikasi SIMAK sudah memiliki UPS atau alat *backup* daya untuk mengamankan server Ketika terjadi daya listrik utama padam, meski begitu UPS belum mengikuti suatu standar keamanan atau belum diperhitungkan waktu ideal untuk dapat mem*backup* server aplikasi SIMAK. Sedangkan untuk keamanan kabel, kabel jaringan dan kabel listrik masih berada diatas lantai. Terkait kebijakan *clear desk* dan *clear screen* masih dilakukan intruksi lisan dari kepala UPTTIK dan belum ada panduan tertulis akan kontrok keamanan tersebut.

Berikut ini adalah Tabel 4.9 hasil perhitungan tingkat kematangan Domain A.11 terkait keamanan fisk dan lingkungan :

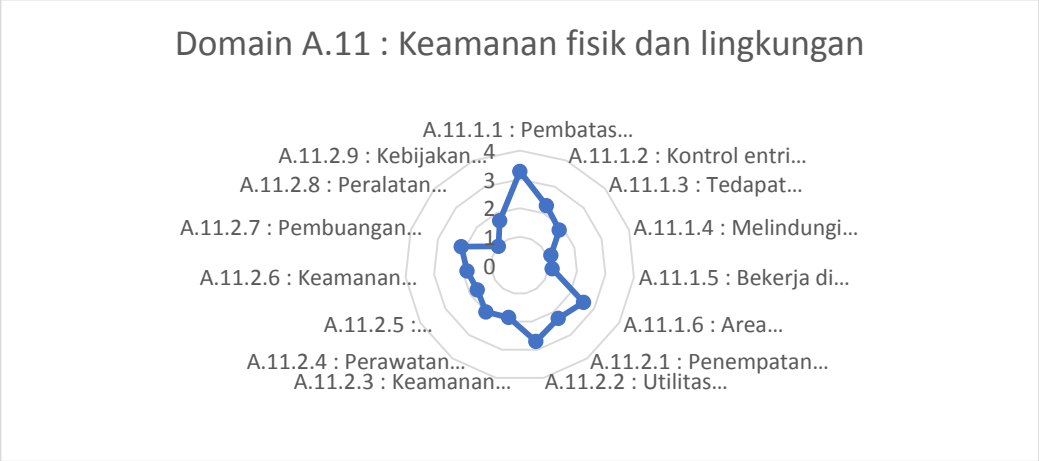
Tabel 4. 9 Hasil perhitungan tingkat kematangan Domain A.11

Domain	Objektif kontrol	Kontrol keamanan	Tingkat kemampauan	Rata-rata objektif kontrol
A.11 : Keamanan fisik dan lingkungan	A.11.1 : Area aman	A.11.1.1 : Pembatas keamanan fisik	3,28	2,04
		A.11.1.2 : Kontrol entri fisik	2,28	
		A.11.1.3 : Tedapat keamanan ruangan dan fasilitas kantor	1,85	
		A.11.1.4 : Melindungi dari ancaman eksternal dan lingkungan	1,14	
	A.11.2 : Peralatan	A.11.2.1 : Penempatan dan perlindungan peralatan	2,28	1,91
		A.11.2.2 : Utilitas pendukung	2,71	
		A.11.2.3 : Keamanan kabel	1,85	
		A.11.2.4 : Perawatan peralatan	2	
		A.11.2.5 : Penghapusan aset	1,71	
		A.11.2.6 : Keamanan peralatan dan aset di luar lokasi	1,85	

Tabel 4. 10 Hasil perhitungan tingkat kematangan Domain A.11 (lanjutan)

Domain	Objektif kontrol	Kontrol keamanan	Tingkat kemampauan	Rata-rata objektif kontrol
		A.11.2.6 : Keamanan peralatan dan aset di luar lokasi	1,85	
		A.11.2.7 : Pembuangan yang aman atau penggunaan kembali peralatan	2,14	
		A.11.2.8 : Peralatan pengguna tanpa pengawasan	1	
		A.11.2.9 : Kebijakan Clear desk and clear screen	1,71	
Tingkat kematangan Domain A.11 Keamanan fisik dan lingkungan				1,97

Hasil perhitungan tingkat kematangan dalam bentuk grafik adalah sebagai berikut :



Gambar 4. 4 Grafik hasil perhitungan tingkat kematangan Domain A.11

5. Hasil pembahasan pemeriksaan keamanan aplikasi SIMAK

Aplikasi SIMAK kerapkali mengalami gangguan keamanan yang terkait dengan keamanan informasi, bedasarkan hasil penelitian yang telah dilakukan salah satu gangguan yang kerap muncul berkaitan dengan Domain A.5 tentang kebijakan keamanan informasi, dimana UPTTIK sebagai penanggungjawab aplikasi SIMAK belum memiliki peraturan tertulis yang menagtur terhadap kebijakan pengelolaan keamanan aplikasi SIMAK.

Kontrol keamanan 9.43 atau yang terkait pengelolaan kata sandi mempunyai nilai kematangan sebesar 1,57 atau berada pada level 2, UPTTIK sebagai yang punya kewajiban memelihara keamanan dalam pengelolaan aplikasi SIMAK belum mempunyai panduan yang mewajibkan pengguna untuk dapat menjaga katasa sandi atau *password* pengguna. Banya pengguna yang tidak menyadari akan pentingnya menjaga kerahasiaan *password* mereka sehingga pada akhirnya mudah bocor ketangan yang tidak bertanggungjawab. Selain daripada itu masih terkait kotrol akses kontrol keamanan 9.2.4 tentang pengelolaan otentikasi rahasia pengguna mendapatkan nilai 1 dan *review* hak akses pengguna hanya mendapatkan nilai 0,57.

Terkait dengan domain 6 atau tentang keamanan informasi organisasi, kontrol keamanan 6.2.2 tentang *teleworking* atau kerja jarak jauh, organisasi belum merinci dan memberikan pengarahan kepada karyawan terkait pentingnya menjaga asset mereka Ketika melakukan *teleworking* atau kerja jarak jauh, diantanya adalah mengunci perangkat, menutup *session* yang sedang aktif. Hal tersebut perlu dilakukan untuk menghindari akses yang tidak sah terhadap server atau aplikasi SIMAK dengan memanfaatkan perangkat atau asset pengguna yang sedang melkukan kerja jarak jauh.

Kontrol keamanan 11.1.4 terkait perlindungan terhadap ancaman eksternal dan lingkungan, ruang server aplikasi SIMAK pada perancangannya tidak dirancang untuk digunakan sebagai ruanagn server, melainkan untuk penggunakaan ruangan kantor pada umumnya, terdapat satu bagian pemisah antara ruangan server dan ruangan rapat utama yang hanya dipisahkan dengan penyekat kaca, ini dapat menjadi risiko akses tidak sah terhdap ruangan server dari orang yang tidak bertanggungjawab.

Dari hasil peritungan tingkat kematangan terkait domain dalam penelitian, dimana *expected maturity* atau kematangan yang menjadi acuan adalah pada level 3 *(define).* Dari ahasil penenelitian yang telah dilakukan diperoleh bahwa rata – rata nilai kematangan adalah pada level 1 *(initial)* yang menandakan bahwa perlu adanya perbaikan dan peningkatan mengingat *expected maturity* adalah pada level 3.

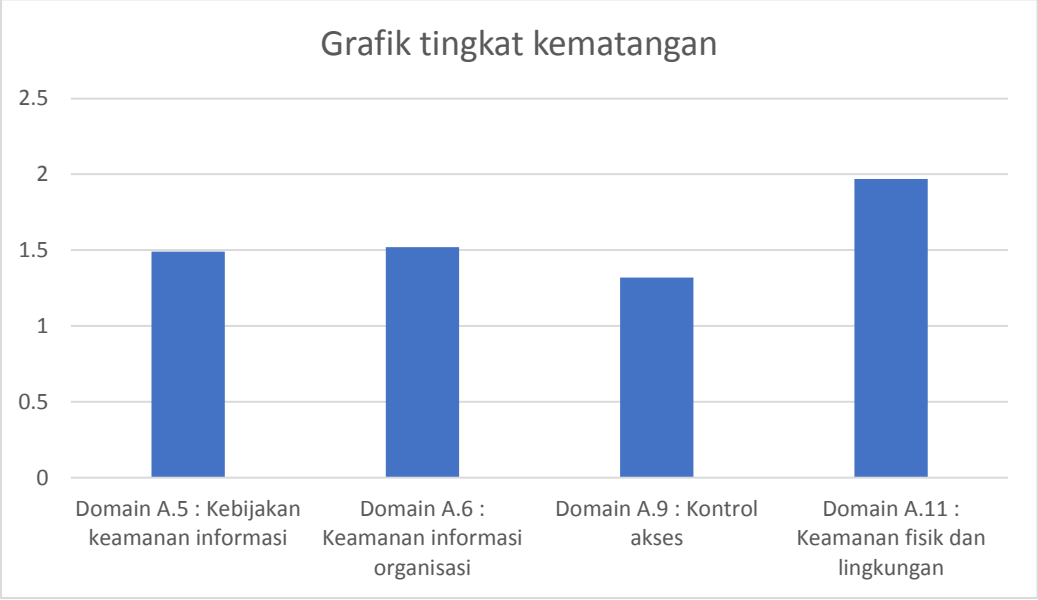
Setelah perhitungan tingkat kematangan pada domain A.5, A.6, A.9, dan A.11 berdasarkan ISO 27002:2013, selanjutnya dapat dilihat rata – rata nilai tingkat kematangan terkait pengelolaan aplikasi SIMAK. Berikut ini adalah tabel 4.10 tentang nilai rata – rata level kematangan terkait domain dalam penelitian :

Tabel 4. 11 Hasil perhitungan tingkat kematangan

Domain	Keterangan	*Index*	*Level*
A.5	Kebijakan keamanan informasi	1,49	1
A.6	Keamanan informasi organisasi	1,52	2
A.9	Kontrol akses	1,32	1
A.11	Keamanan fisik dan lingkungan	1,97	2
Rata – rata tingkat kematangan		1,57	2

Dari tabel 4.9 diartikan bahwa level kematangan sebesar 1,57 atau berada pada level 2 *(repeatable)* yang juga dapat diartikan bahwa pengelolaan aplikasi SIMAK sudah dijalankan berdasarkan ketentuan dasar namun belum terdokumentasi.

Dari tabel 4.9 maka dapat ditampilkan dalam grafik adalah sebagai berikut :



Gambar 4. 5 Grafik tingkat kematangan

4.5. Analisis Kesenjangan

Setelah melakukan perhitungan tingkat kematangan analisis tingakat keamanan aplikasi SIMAK memilki nilai 1,57 *(repeatable)* atau berada pada level 2 dan level

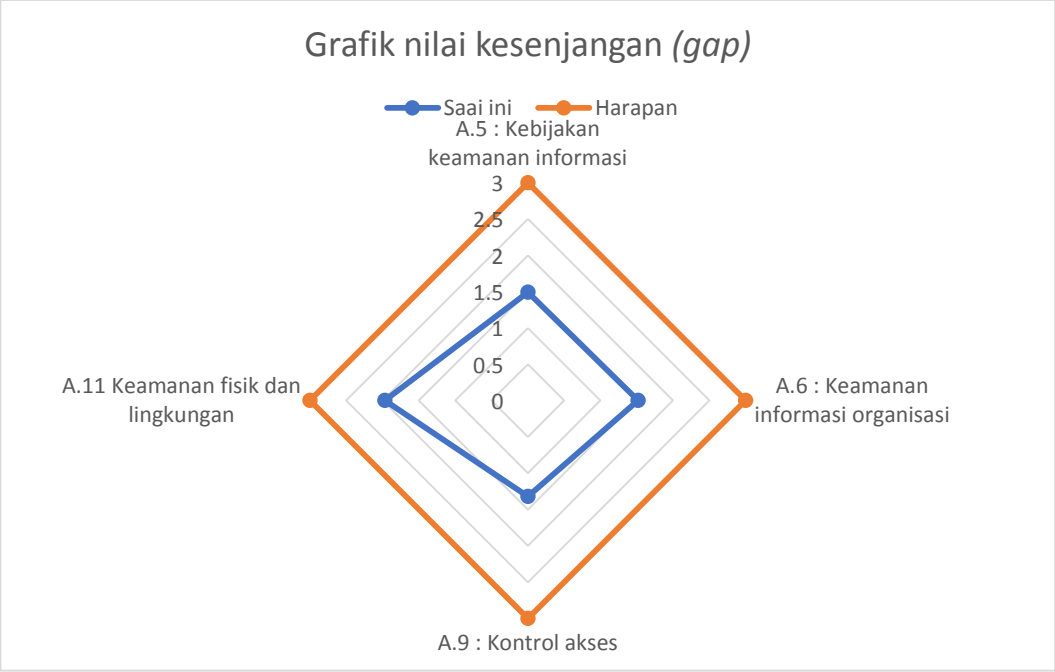
kematangan yang diharapkan berdasarakan hasil wawancara dengan kepala UPTTIK adalah level 3 atau *define.* Berikut adalah Tabel 4.10 tentang perhitungan kesenjangan :

Tabel 4. 12 Tabel kesenjangan antara kondisi saat ini dengan kondisi harapan

Domain	Keterangan	*Maturity level*		Kesenjangan
		Saat ini	Harapan	
A.5	Kebijakan keamanan informasi	1,49	3	1,51
A.6	Keamanan informasi organisasi	1,52	3	1,48
A.9	Kontrol akses	1,32	3	1,68
A.11	Keamanan fisik dan lingkungan	1,97	3	1,03
Rata - rata kesenjangan				1,42

Dari tabel 4.10 dapat dilihat, nilai kesenjangan atau *gap* antara kondisi *existing* atau kondisi saat ini dengan *potential* atau kondisi harapan untuk masing – masing domain adalah Domain A.5 bernilai 1,51, Domain A.6 bernilai 1,48, Domain A.9 berniali 1,68, dan Domain A.11 bernilai 1,03.

Selanjutnaya dari amasing – masing nilai di hitung rata – rata kesenjangannya dan smenghasilakan nilai 1,42 atau berada pada level 1 *(initial).* Tingkat kesenjangan digambarkan dalam gambar 4.6 berikut ini :



Gambar 4. 6 Gambar tingkat kesejnagan kondisi saat ini dan kondisi harapan

Pada gambar 4.6, kondisi saat ini gambarkan dengan garis berwarna biru, kondisi harapan atau kondisi potensial tunjukan dengan garis berwarna merah. Secara terperinci dapat jelaskan kesenjangan masing – masing domain yaitu Domain A.5 mempunyai nilai kesenjangan sebesar 1,51, Domain A.6 mempunyai nilai kesenjangan sebesar 1,48, Domain A.9 mempunyai nilai kesenjangan 1,68 dan Domain A.11 mempunyai nilai kesenjangan sebesar 1,03, sedangkan nilai kesenjangan terbesar adalah pada Domain A.9 atau terkait kontrol akses. Secara singkat dapat dikatakan, semakin besar nilai kesenjangan suatu domain, maka kemungkinan terjadi penyimpangan pun akan semakin tinggi.

4.6. Rekomendasi

Tabel 4. 13 Hasil temuan dan rekomendasi Domain A.5

Domain	Objektif kontrol	Kontrol keamanan	Temuan	Rekomendasi
A.5 : Kebijakan Keamanan Informasi	A.5.1 : Arahan manajemen untuk keamanan informasi	A.5.1.1 : Kebijakan untuk keamanan informasi	Kebijakan informasi sudah ada, namun masih bersifat lisan disampaikan kepada karyawan UPTTIK oleh kepala UPT.	Membuat kebijakan secara tertulis terkait kebijakan keamanan informasi, untuk menjadi guide line bagi karyawan.

Tabel 4. 14 Hasil temuan dan rekomendasi Domain A.6

Domain	Objektif kontrol	Kontrol keamanan	Temuan	Rekomendasi
A.6 : Keamanan Informasi Organisasi	A.6.1 : Internal Organisasi	A.6.1.1 : Peran dan tanggung jawab keamanan informasi	Peran dan tanggungjawab terhadap keamanan informasi sudah dilakukan oleh organisasi, namun hanya bersifat lisan dan belum memiliki dokumen panduan, dari penelitian juga diketahui bahwa tidak semua karyawan faham terkait peran dan perlindungan keamanan informasi organisasi.	Mengimplementasikan setiap peraturan yang sudah dibuat, mengkomunikasikan kepada setiap pengguna (karyawan) terkait perlindungan keamanan informasi.

Tabel 4. 15 Hasil temuan dan rekomendasi Domain A.9

Domain	Objektif kontrol	Kontrol keamanan	Temuan	Rekomendasi
A.9 : Kon akses	A.9.1 : Persyaratan bisnis untuk kontrol akses	A.9.1.1 : Kebijakan kontrol akses	Kebiajakn terkait kontrol akses terhadap aplikasi SIMAK diatur berdasarkan kebijakan yang dikeluarkan oleh pimpinan UPTTIK, kebijakan belum tertulis, dan masih berupa arahan secara lisan dari pimpinan, kebijakan belum mengacu pada suatu standar, kebijakan dikeluarkan berdasarkan kebiasaan yang diwariskan dari kepemimpinan terdahulu.	Organisasi harus membuat panduan terkait kontrol akses, panduan harus berisikan tentang mekanispe atau tatacara yang mengatur tentang kontrol akses terhadap aplikasi SIMAK, pengguna khusus diwajibkan faham terkait menjaga keamanan data dan kontrol akses terhadap aplikasi SIMAK.

Tabel 4. 16 Hasil temuan dan rekomendasi Domain A.11

Domain	Objektif kontrol	Kontrol keamanan	Temuan	Rekomendasi
A.11 : Keamanan f dan lingkung	A.11.1 : Area aman	A.11.1.1 : Pembatas keamanan fisik	Perimeter atau pembatas keamanan fisik telah ada untuk mengamankan server aplikasi SIMAK, pebatas keamanan tersebut berupa kunci pintu sidik jari, tidak hanya satu tetapi terdapat 3 lapis perimeter keamanan, dua diantaranya menggunakan sidik jari, ruangan server aplikasi SIMAK juga di kelilingi oleh dinding beton, namun ada beberap bagian dari ruangan server yang berbatasan langsung denagan ruangan lain yang hanya di batasi oleh dinding kaca biasa,	Perimeter pembatas fisik harus *direview* secara berkala, seluruh pembatas keamaman fisk harus berdasarkan standar ruangan server.

BAB V

PENUTUP

5.1. Kesimpulan

Penelitain yang dilakukan peneliti terkait analisis tingkat keamanan aplikasi SIMAK medapatkan hasil sebagai berikut :

1. ISO 27002:2013 adalah sebagai acuan dalam menjaga keamanan informasi bedasarakan peraturan, risiko, hukum, kebutuahan dan tujuan informasi pada aplikasi SIMAK. Dari hasil penelitian penerapan standarisasi ISO 27002:2013 pada aplikasi SIMAK belum mencapai target terhadap kondisi yang diharapkan, perlu dilakukan peningkatan dan pemeliharaan terkait domain yang telah ditentukan dalam penelitian.
2. *Maturity level* atau tingkat kematangan aplikasi SIMAK masing – masing domain adalah domain A.5 kebijakan keamanan informasi berada pada level 1 *(initial),* domain A.6 keamanan informasi organisasi berada pada level 2 *(repeatable),* domain A.9 kontrol akses berada pada level 1 *(initial)* dan domain A.11 keamaman fisik dan lingkungan berada pada level 2 *(repeatable).*
3. Terdapat banyak kontrol keamanan yang belum terdokumentasi atau belum tertulis, terdapat kontrol keamanan yang dilakukan berdasarkan kebiasaan dan bukan mengacu pada suatu standar baku.

5.2. Saran

Dari hasil penelitian yang telah dilakukan, saran yang dapat diberikan kepada UPTTIK sebagi penanggungjawab dan pengelola aplikasi SIMAK supaya mendapatakan atau tercipta aplikasi SIMAK yang berjalan berdasarkan standar yang telah ditentukan yaitu ISO 27002:2013 adalah sebagai beikut :

1. Bagi UPTTIK sebagai pengelola aplikasi SIMAK diharapkan untuk melakukan perbaikan dalam tatakelola aplikasi SIMAK, membuat peratuaran terkait tatakelola aplikasi SIMAK, membuat aturan tertulis dan prosedur keamanan terkait

pengelolaan aplikasi SIMAK supaya risiko dan ancaman keamanan dapat diminimalisir atau dihindari.

2. Bagi UPTTIK sebagai pengelola dan penanggungjawab aplikasi untuk dapat melakukan audit secara keseluruhan terkait pengelolaan aplikasi SIMAK menggunakan keseluruhan domain pada ISO 27002:2013 hal ini dilakukan supada risiko terkalit keamanan informasi pada pengelolaan aplikasi SIMAK bisa lebih diminimalisir dan keamanan data pengguna dapat lebih terjamin.

DAFTAR PUSTAKA

A Hall, James. 2011. *Accounting Information System.* Edisi ke 4, Salemba Empat. Jakarta.

Amarusu. 2013. Sistem informasi Akadmik sekolah. Medan.

Apriandari, Ashwin Sasongko. 2018. Analisis Sistem Manajemen Keamanan Informasi Menggunakan SNI ISO/IEC 27001:2013 Pada Pemerintahan Daerah Kota Sukabumi (Studi Kasus: Di Diskominfo Kota Sukabumi). Vol. 8 No. 1. SANTIKA.

Altry David Purba, I Ketut Adi Purnawan, I Putu Eka Pratama. 2018. Audit Keamanan TI Menggunakan Standar ISO/IEC 27002 dengan COBIT 5. Vol. 6, No. 3.

Ririh Riswaya, Asep, Ashwin Sasongko, dan Asep Maulana. 2020. Evaluasi Tata Kelola Keamanan Teknologi Informasi Menggunakan Indeks KAMI untuk Persiapan Standar SNI ISO/IEC 27001. Vol.14, No. 1.

Desak Made Novita, IMade Surasa, dan I Ketut Adi Purnawan. 2019. Mengetahui Tingkat Kematangan Aplikasi pada Start up IT Menggunakan Metode CMMI dan TMMi. Vol. 7, No. 1.

Direktorat Keamanan Informasi. 2011. Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik. Jakarta: Kementrian Keamanan Informasi dan Informatika RI.

Endang Kurniawan, dan Imam Riadi. 2018. Analisis Tingkat Keamanan Sistem Informsi Akademik Bderdasarkan Standar ISO 27002:2013 Menggunakan SSE-CMM. Vol. 2, No. 1.

Fauzi. 2018. Implementasi Awal Sistem Manajemen Keamanan Informasi pada UKM Menggunakan Kontrol ISO/IEC 27002. JTERA - Jurnal Teknologi Rekayasa, Vol. 3, No. 2.

Febrianto, dan Dana Indra Sensuse. 2017. Evaluasi Keamanan Informasi Menggunakan ISO/IEC 27002: Studi Kasus Pada Stimik Tunas Bangsa Banjarnegara. INFOKAM.

Halim, Merliana, dan Tanuwijaya. 2012. Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27002 (Studi Kasus: PT. Aneka Jaya Baut Sejahtera). Jurnal JSIKA.

Hermaduanti, dan Imam Riadi. 2016. *Automation framework for rogue access point mitigation in IEEE* 802.1X-based WLAN. Journal of Theoretical and Applied Information Technology.

Hutahaean. Jeperson. 2014. "Konsep Sistem Informasi", 1th ed. Budi Utama. Yogyakarta.

Krismaji, 2015. Sistem Informasi Akuntansi, Edisi Ketiga, Sekolah Tinggi Ilmu Manajemen, Yogyakarta.

McGraw. 2006. *Software Security:Building Security In. Addison-Wesley.*

Made Novita, I Made Sukarsa, I Ketut Adi Purnawan. 2019. Mengetahui Tingkat Kematangan Aplikasi pada *Start up* IT Menggunakan Metode CMMI dan TMMi. MERPATI VOL. 7, NO. 1.

Nugroho, Anggun. 2015. Perancangan Sistem Informasi Pengelolaan UKM STIMIK STIKOM Bali Berbasis Client Server, Konferensi Nasional Sistem & Informatika.

O'Brien, A. James. G. M. Marakas. 2016. Analisa Sistem Informasi, Ed 1, Andy, Yogyakarta.

Riadi, Imam, Jazi Eko Istiyanto, Ahmad Ashari and Subanar. 2013. *"Internet Forensics Framework Based-on Clustering" International Journal of Advanced Computer Science and Applications* (IJACSA), 4(12).

Rosmiati, Riadi, Imam. & Prayudi, Yudi. 2016. *A Maturity Level Framework for Measurement of Information Security Performance. International Journal of Computer Applications*. 141. 975-8887. 10.5120/ijca2016907930, Yogyakarta.

Rusyudi Umar, Imam Riadi, dan Eko Handoyo. 2019. Analisis Sistem Keamanan Informasi Berdasarkan *Framework* COBIT 5 Menggunakan *Capability maturity Model Integration* (CMMI).

Rutanaji, Sri Suning Kusumawardani, dan Wing Wahyu Winarno. 2018. Penggunaan Kerangka Kerja SNI ISO/IEC 27001:2013 Untuk Implementasi Tata Kelola Keamanan Informasi Arsip Digital Pemerintah Berbasis Komputasi Awan (Arsip Nasional RI) ISSN: 2580-8796.

Sakinah, Faroh, Setiawan, Bambang. 2014. Indeks Penilaian Kematangan (Maturity) Manajemen Layanan TI. Vol.3, No. 2.

Sarno, Iffano. 2009. Sistem Manajemen Keamanan Informasi. ITS Press. Surabaya.

Stair, R, Reynolds, G, 2012. *Principles of Information System, Tenthh Edition,* Nelsol Education, Boston.

Sugiyono, 2011. Metode Penelitian Bisnis, Edisi 2, CV. Alfabeata. Bandung.

Tanuwijaya, H. dan Sarno, R. 2010. *Comparation of CobiT Maturity Model and Structural Equation Model for Measuring the Alignment between University Academic Regulati ons and Information Technology Goals, International Journal of Computer Science and Network Security*, VOL.10 No.6, Surabaya.

Apriandari, Winda dan Ashwin Sasongko. 2018. Analisis Manajemen Keamanan Informasi Menggunakan SNI ISO/IEC 27001:2013 Pada Pemerintahan Daerah Kota Sukabumi. Vol.8, No.2.

Yakub, 2012. Pengantar sistem informasi, Edisi 1, Graha Ilmu, Yogyakarta.

DAFTAR LAMPIRAN

LAMPIRAN A

Tabel lampiran A. 1 Perhitunagn tingkat kematangan

Domain	Keterangan	Maturity level		Kesenjangan
		Saat ini	Harapan	
A.5	Kebijakan keamanan informasi	1,49	3	1,51
A.6	Keamanan informasi organisasi	1,52	3	1,48
A.9	Kontrol akses	1,32	3	1,68
A.11	Keamanan fisik dan lingkungan	1,97	3	1,03
Rata - rata kesenjangan				1,42

Tabel lampiran A. 2 Domain A.5 Kebiajakan keamanan informasi

Domain	Objektif kontrol	Kontrol keamanan	Kemampauan	Rata-rata objektif konrol
A.5 : Kebijakan Keamanan Informasi	A.5.1 : Arahan manajemen untuk keamanan informasi	A.5.1.1 : Kebijakan untuk keamanan informasi	1,85	1,49
		A.5.1.2 : *Review* kebijakan untuk keamanan informasi	1,14	
Rata – rata level kematangan domain A.5 Kebijakan keamanan informasi				1,49

Tabel lampiran A. 3 Domain A.6 Keamanan informasi oraganisasi

Domain	Objektif kontrol	Kontrol keamanan	Kemampauan	Rata-rata objektif konrol
A.6 : Keamanan Informasi Organisasi	A.6.1 : Internal Organisasi	A.6.1.1 : Peran dan tanggung jawab keamanan informasi	2,14	1,56
		A.6.1.2 : Pemisahan tugas	2	
		A.6.1.3 : Kontak dengan pihak berwenang	1,28	
		A.6.1.4 : Kontak dengan kelompok minat khusus	1	
		A.6.1.5 : Keamanan informasi dalam manajemen proyek	1,42	
	A.6.2 : Perangkat Seluler dan *Teleworking*	A.6.2.1 : Kebijakan perangkat seluler	1,42	1,49
		A.6.2.2 : *Teleworking*	1,57	
Rata – rata level kematangan domain A.6 Keamanan informasi organisasi				1,52

Tabel lampiran A. 4 Domain A.9 Kontrol akses

Domain	Objektif kontrol	Kontrol keamanan	Kemampauan	Rata-rata objektif konrol
A.9 : Kontrol akses	A.9.1 : Persyaratan bisnis untuk kontrol akses	A.9.1.1 : Kebijakan kontrol akses	1,57	1,35
		A.9.1.2 : Akses ke jaringan dan layanan jaringan	1,14	
	A.9.2 : Manajemen akses pengguna	A.9.2.1 : Pendaftaran dan pencabutan akses pengguna	1,57	1,47
		A.9.2.2 : Penyediaan akses pengguna	2,28	
		A.9.2.3 : Pengelolaan hak akses istimewa	2	
		A.9.2.4 : Pengelolaan informasi otentikasi rahasia pengguna	1	
		A.9.2.5 : *Review* hak akses pengguna	0,57	
		A.9.2.6 : Penghapusan atau penyesuaian hak akses	1,42	
	A.9.3 : Tanggung jawab pengguna	A.9.3.1: Penggunaan informasi otentikasi rahasia	0,71	0,71
	A.9.4 : Kontrol akses sistem dan aplikasi	A.9.4.1 : Pembatasan akses informasi	1,71	1,76
		A.9.4.2 : Amankan prosedur log-on	1,85	
		A.9.4.3 : Sistem manajemen kata sandi	1,57	
		A.9.4.4 : Penggunaan program utilitas dengan hak istimewa	1,57	
		A.9.4.5 : Kontrol akses ke kode sumber program	2,14	
Rata – rata level kematangan domain A.9 Kontrol akses				1,32

Tabel lampiran A. 5 Doamain A.11 Keamanan fisik dan lingkungan

Domain	Objektif kontrol	Kontrol keamanan	Kemampauan	Rata-rata objektif konrol
A.11 : Keamanan fisik dan lingkungan	A.11.1 : Area aman	A.11.1.1 : Pembatas keamanan fisik	3,28	2,04
		A.11.1.2 : Kontrol entri fisik	2,28	
		A.11.1.3 : Tedapat keamanan ruangan dan fasilitas kantor	1,85	
		A.11.1.4 : Melindungi dari ancaman eksternal dan lingkungan	1,14	
		A.11.1.5 : Bekerja di tempat yang aman	1,14	
		A.11.1.6 : Area pengiriman dan pemuatan	2,57	
	A.11.2 : Peralatan	A.11.2.1 : Penempatan dan perlindungan peralatan	2,28	1,91
		A.11.2.2 : Utilitas pendukung	2,71	
		A.11.2.3 : Keamanan kabel	1,85	
		A.11.2.4 : Perawatan peralatan	2	
		A.11.2.5 : Penghapusan aset	1,71	
		A.11.2.6 : Keamanan peralatan dan aset di luar lokasi	1,85	
		A.11.2.7 : Pembuangan yang aman atau penggunaan kembali peralatan	2,14	
		A.11.2.8 : Peralatan pengguna tanpa pengawasan	1	
		A.11.2.9 : Kebijakan Clear desk and clear screen	1,71	
Rata – rata level kematangan domain A.11 : Keamanan fisik dan lingkungan				1,97

LAMPIRAN B

Tabel lampiran B. 1 Domain A.11 Keamanan fisik dan lingkungan

Domain A.5 : Kebijakan keamanan informasi																	
Domain A.5.1 : Arahan manajemen untuk keamanan informasi																	
Domain A.5.1.1 : Kebijakan untuk keamanan informasi																	
No	Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
1	Terdapat kebijakan keamanan informasi terkait pengolahan informasi	Kebijakan informasi sudah ada, namun masih bersifat lisan disampaikan kepada karyawan UPTTIK oleh ketua.	0	2	4	1	0	0	7	0	2	8	3	0	0	13	1,85

LAMPIRAN C

Tabel lampiran C. 1 Temuan dan Rekomendasi

Domain	Objektif kontrol	Kontrol keamanan	Temuan	Rekomendasi
A.5 : Kebijakan Keamanan Informasi	A.5.1 : Arahan manajemen untuk keamanan informasi	A.5.1.1 : Kebijakan untuk keamanan informasi	Kebijakan informasi sudah ada, namun masih bersifat lisan disampaikan kepada karyawan UPTTIK oleh ketua.	Membuat kebijakan secara tertulis terkait kebijakan keamanan informasi, untuk menjadi guide line bagi karyawan.
		A.5.1.2 : *Review* kebijakan untuk keamanan informasi	*Review* kebijakan untuk kemanan informasi tidak dilakukan secara berkala, namun hanya dilakukan apabila terjadi atau ditemukan perubahan situasi terkait keamanan informasi	Mengkaji kebijakan yangsudah ada secara terjadwal dan diimplementasikan dalam bentuk peraturan tertulis.
A.6 : Keamanan Informasi Organisasi	A.6.1 : Internal Organisasi	A.6.1.1 : Peran dan tanggung jawab keamanan informasi	Peran dan tanggungjawab terhadap keamanan informasi sudah dilakukan oleh organisasi, namun hanya bersifat lisan dan belum memiliki dokumen panduan, dari penelitian juga diketahui bahwa tidak semua karyawan faham terkait peran dan perlindungan keamanan informasi organisasi.	Mengimplementasikan setiap peraturan yang sudah dibuat, mengkomunikasikan kepada setiap pengguna (karyawan) terkait perlindungan keamanan informasi.
		A.6.1.2 : Pemisahan tugas	Mekanisme pemisahan tugas sudah dilakukan secara tertulis namun belum terdokumentasi, masing - masing karyawan ditempatkan pada bagian masing - masing berdasarkan keahlian masing - masing.	Membuat dokumentasi terkait pemisahan tugas setiap karyawan, pemisahan tugas dan pendokumentasian diharapkan tidak adanya tumpang tindih dalam hal pengelolaan tugas.

Tabel lampiran C. 2 Temuan dan Rekomendasi (Lanjutan)

Domain	Objektif kontrol	Kontrol keamanan	Temuan	Rekomendasi
		A.6.1.3 : Kontak dengan pihak berwenang	Terkait dengan terjadinya suatu insiden terdapat mekanisme atau alur dalam penanggulangan masalah, contohnya terjadi masalah pada server aplikasi SIMAK yang menyebabkan berhentinya aplikasi, namun mekanisme dilakukan secara kebiasaan dan belum mengikuti suatu panduan dan belum terdokumentasi.	Membuat panduan terkait alur penanganan insiden keamanan informasi terkait peanganan aplikasi SIMAK, dan server aplikasi SIMAK.
		A.6.1.4 : Kontak dengan kelompok minat khusus	Masing - masing karyawan mempunyai tugas dan fungsi yang berbeda, termasuk dalam hal kontak dengan grup atau komunitas khusus terkait dengan keamanan informasi, misalnya karyawan bagian developer SIMAK ditugaskan oleh pimpinan dalam meningkatkan pengetahuan dalam hal pengembangan aplikasi.	Organisasi harus membuat dokumentasi terkait kontak dengan komunitas atau group khusus seperti pelatihan untuk setiap keahlian dari masing - masing karyawan.
		A.6.1.5 : Keamanan informasi dalam manajemen proyek	Penilaian terkait keamanan dalam proyek dilakukan, namun tidak rutin, penilaian hanya dilakukan apabila ditemukan suatu kejadian terkait keamanan, selain itu juga belum terdokumentasi dengan baik. Penilaian keamanan belum mengacu pada suatu panduan secara resmi, hanya berdasarkan pengalaman dari karyawan yang menilai.	UPTTIK harus mempunyai panduan khusu terkait penilaian keamanan dalam suatu proyek, membuat dokumentasi terkait penanganan penilaian keamanan proyek, penilaian keamanan harus berdasarkan suatu standar. Selanjutnya dibaut kedalam suatu panduan khusu terkait penannganan dan penilaian keamanan proyek.

Tabel lampiran C. 3 Temuan dan Rekomendasi (Lanjutan)

Domain	Objektif kontrol	Kontrol keamanan	Temuan	Rekomendasi
	A.6.2 : Perangkat Seluler dan *Teleworking*	A.6.2.1 : Kebijakan perangkat seluler	Kebijakan terkait perangkat selular hanya berupa himbauan keamanan, berupa banner yang berisi saran agar berhati - hati dalam pengaksesan jaringan dan installasi program. Banner himbauan disebarkan ke seluruh fakultas yang ada di Universitas Siliwangi.	UPTTIK secara rutin harus menginformasikan kepada penggguna tekait keamanan jaringan dan perangkat selular, informasi dapat berupa pamplet dan pelatihan secara langsung.
		A.6.2.2 : *Teleworking*	Tedapat kebijakan bagi karyawan yang an melakukan *teleworking* atau kerja jarak jauh, manajemen tidak memberikan arahan secara lengkap terkait dengan keamanan lingkungan yang dijadikan *teleworking*, jaringan yang dipakai untuk mengakases server aplikasi SIMAK. karyawan yang melakukan *teleworking* juga tidak melakukan dokumentasi tentang hasil kerjanya.	UPPTIK harusmerikan membuat panduan yang dapat digunakan untuk pengguna aplikasi SIMAK terkait *teleworking*, panduan tersebut harus berisi tentang panduan menjaga keamanan asset priabadi, pemilihan lokasi *teleworking* dan penggunaan jaringan yang akan digunakan untuk mengakses aplikasi atau server SIMAK, karyawan dengan akses klusus harus menggunakan VPN ketika mengakses server SIMAK.

Tabel lampiran C. 4 Temuan dan Rekomendasi (Lanjutan)

Domain	Objektif kontrol	Kontrol keamanan	Temuan	Rekomendasi
A.9 : Kontrol akses	A.9.1 : Persyaratan bisnis untuk kontrol akses	A.9.1.1 : Kebijakan kontrol akses	Kebiajakn terkait kontrol akses terhadap aplikasi SIMAK diatur berdasarkan kebijakan yang dikeluarkan oleh pimpinan UPTTIK, kebijakan belum tertulis, dan masih berupa arahan secara lisan dari pimpinan, kebijakan belum mengacu pada suatu standar, kebijakan dikeluarkan berdasarkan kebiasaan yang diwariskan dari kepemimpinan terdahulu.	Organisasi harus membuat panduan terkait kontrol akses, panduan harus berisikan tentang mekanispe atau tatacara yang mengatur tentang kontrol akses terhadap aplikasi SIMAK, pengguna khusus diwajibkan faham terkait menjaga keamanan data dan kontrol akses terhadap aplikasi SIMAK.
		A.9.1.2 : Akses ke jaringan dan layanan jaringan	Karyawan yang bertugas sebagai programmer menggunakan jaringan privat dalam mengakases server aplikasi SIMAK, hal ini diatur oleh kebijakan yang keluarkan oleh pimpinan UPTTIK, namun begitu kebijakan dan akses belum terdokumentasi dengan baik. Sedangkan bagi karyawan yang hanya berhak mengakses aplikasi SIMAK dengan level biasa bisa menggunakan jaringan yang digunakan pengguna seca umum.	Diperlukan pendokumentasian terkait akses terhadap jaringan dan server aplikasi SIMAK, karyawan yang mempunyai akses khusus terhadap aplikasi, server SIMAK harus menggunakan jaringan khusus dan faham tentang penanganan keamanan jaringan yang digunakannya.

Tabel lampiran C. 5 Temuan dan Rekomendasi (Lanjutan)

Domain	Objektif kontrol	Kontrol keamanan	Temuan	Rekomendasi
	A.9.2 : Manajemen akses pengguna	A.9.2.1 : Pendaftaran dan pencabutan akses pengguna	Proses pendafran dan bencabuatan hak akses bagi pengguna sudah dilakukan, pengguna yang berpindah unit kerja di cabut hak aksesnya terhadap aplikasi SIMAK (pemrosesan data) dan hanya dapat mengakses aplikasi sesuai dengan unit kerja barunya, juga terhadap server, dicabut atau diahapus, pendaftaran, pencabutan atau pembatalan hak akses dilakukan oelh superadmin berdasarkan arahan dari kepala UPTTIK. Namun begitu tahapan atau langkah ini belum terdokumentasi dengan baik.	Pendokumentasian terkait pendaftaran dan pencabutan hak akses perlu dilakukan, karyawan yang berwenang mendaftrkan dan mencabut akses pengguna harus mendokumentasikan apa yang dikerjakannya. *Review* pencabutan dan pendaftaran hak akses pengguna harus rutin dilakukan untuk mencegah akses ilegal, diperlukan panduan secara tertulis terkait pencabutan dan pendaftaran akses bagi pengguna.
		A.9.2.2 : Penyediaan akses pengguna	Penyediaan akases pengguna dilakukan oleh pemegang sistem, seperti pengguna (karyawan) baru di daftarkan terhadap sistem atau aplikasi SIMAK, pemegang sistem mem-verifikasi tingkat atau hak akses karayawan baru tersebut, level akses di cocokan dengan tugas dan fungsi karyawan sesuai dengan surat keputusan yang ia miliki sebagai pegawai. Proses ini dilakukan secara formal oleh pemilik akses utama.	Penyediaan akses bagi pengguna sudah berdasarkan surat keputusan yang dikeluarkan oleh kepegawaian dan dilakukan pendaftaran oleh karyawan yang sesuai dari bagaian UPTTIK. Namun pendokumentasian masih belum dilakukan oleh pengguna dalam melakukan skegiatannya.

Tabel lampiran C. 6 Temuan dan Rekomendasi (Lanjutan)

Domain	Objektif kontrol	Kontrol keamanan	Temuan	Rekomendasi
		A.9.2.3 : Pengelolaan hak akses istimewa	Pengeloaan super admin dilakukan berdasarkan tugas dan fungsi karayawan, tidak semua karyawan UPTTIK mempunyai hak akses sebagai super admin pada aplikasi maupun server aplikasi SIMAK, penentuan akses sebagai super admin dapat dilakukan juga terkait kebutuhan tertentu, misalnya bagian akademik memerlukan akses terkait pengelolaan suatu data, maka akses dapat dibuat berdasarkan surat keterangan.	Hk istimewa sudah disediakan dan diberikan secara tepat kepada orang - orang yang berkepentingan di UPTTIK, perlunya dilakukan pemantauan terhadap akses khusus, pendokumentasian terkait akses kusus harus dilakukan secara rutin dan teratur.
		A.9.2.4 : Pengelolaan informasi otentikasi rahasia pengguna	Pengelolaan informasi rahasia sudah dilakukan, karyawan di UPTTIK harus menjaga data sensitif dan juga dilarang membagikan data yang bersifat sensitif atau arahasia kepada piahak luar, namun meski begitu, belum ada dokumentasi dan peraturan secara tertulis terkait kebijakan tersebut.	UPTTIK harus membuat dokumen perjadjian secara tertulis yang bermaterai terkait komitmen menjaga kearahasiaan data yang berada di UPTTIK, seluruh anggota atau karyawan UPTTIK harus berkomitmen dalam menjaga data rahasia yang diolah d UPTTIK.

Tabel lampiran C. 7 Temuan dan Rekomendasi (Lanjutan)

Domain	Objektif kontrol	Kontrol keamanan	Temuan	Rekomendasi
		A.9.2.5 : *Review* hak akses pengguna	Terkait hak akses pengguna, tidak ada mekanisme yang mengatur bahwa UPTTIK sebagai pemegang sistem atau aplikasi SIMAK harus meninjau atau me-*review* hak aksesnya, namun peninjauan dilakukan berdasarkan ajuan dari pengguna. Proses peninjauan dilakukan secara tidak rutin dan belum ada dokumentasi terkait hal itu.	Pemegang sistem atau aplikasi SIMAK harus melakukan *review* terhadap akses pengguna secara rutin, memastikan hak akses pengguna sudah sesuai dengan hak akses dan kewenanganya masing masing.
		A.9.2.6 : Penghapusan atau penyesuaian hak akses	Ketika seorang karyawan tidak lagi bekerja pada suatu bagian, maka akses terhadap aplikasi SIMAK juga di cabut, begitu juga ketika pengguna pindah ke bagian lain, maka hak akses terhadap aplikasi SIMAK di sesuaikan sesuai dengan ketentuan yang baru.	*Review* secara rutin harus dilakukan terkait dengan penyesuaian hak akses pengguna yang berpindah unit kerja untuk dapat menyesuaikan akses barunya, selain itu juga akses ilegal terkait abatasan hak akses harus diperhatiakan dan didokumentasikan.
	A.9.3 : Tanggung jawab pengguna A.9.4 : Kontrol akses sistem dan aplikasi	A.9.3.1: Penggunaan informasi otentikasi rahasia	Terkait pengelolaan data rahasia pada aplikasi SIMAK, UPTTIK belum mempunyai dokumen yang mengatur hal itu, namun segala bentuk pengelolaan data sensitif atau rahasia tetap dilakukan, namun hanya berdasarkan arahan kepala UPTTIK, proses pengelolaan dilakukan belum terdokumentasi.	Perlu dibuat dokumen perjanjian yang ditandatangani oleh karayawan UPTTIK terkait pengelolaan data dan dokumen rahasia, perlu di buat dokumentasi terkait pengelollan dokumen rahasia yang dilakukan oleh karyawan UPTTIK.

Tabel lampiran C. 8 Temuan dan Rekomendasi (Lanjutan)

Domain	Objektif kontrol	Kontrol keamanan	Temuan	Rekomendasi
		A.9.4.1 : Pembatasan akses informasi	Akses terhadap aplikasi SIMAK dibatasi sesuai dengan kebutuhan dan kebijakan organisasi, kebijakan tersebut berupa kebijakan lisan yang diterjemahkan dari peraturan atau kebijakan pimpinan. Pembatasan akses dilakukan oleh pemegang sistem, pembatasan belum terdokumentasi.	Perlu dibuat peraturan secara tertulis terkait pembatasan dan kewenangan akses terhadap hak akses aplikasi SIMAK, perlu penerjemahan terkait posisi atau jabatan anggota atau pengguna untuk diimplementasikan dalam penyesuaian akses atau pembatasan aplikasi SIMAK.
		A.9.4.2 : Amankan prosedur log-on	Aplikasi SIMAK diamankan oleh prosedur log-on, dimana prosedur log-on ini mengharuskan pengguna untuk login terhadap aplikkasi SIMAK untuk dapat mengakses data atau mengolah data didalamnya. Prosedur ini dilakukan untuk mngamankan data dari akses yang tidak sah.	Prosedur logon sudah tersdia pada aplikasi SIMAK untuk mengamankan data dan sebagai perlindungan dari akses luar atau akses yang tidak sah
		A.9.4.3 : Sistem manajemen kata sandi	Manajemen pengolahan kata sandi aplikasi SIMAK masih menerima password dengan karakter sederhana, sistem belum dirancang untuk mengharuskan pengguna menggunakan atu menginputkan kata sandi yang rumit misalnya kombinasi antara huruf, angka dan simbol, hal ini bisa jadi kelemahan yang dapat berisiko terhdapat keamanan data.	Aplikasi SIMAK harus diperbaharui sehingga mewajibakan penggunanya menggunakan katasandi yang rumit, UPTTIK aharus membuat kebijakan tertuis terkait perlindungan kata sandi dan mewajibakan pergantaian katasandi secara rutin, UPTTIK harus memberi penyuluhan atau pelatihan terkait pentingnya menjaga atau mengamankan kata sandi.

Tabel lampiran C. 9 Temuan dan Rekomendasi (Lanjutan)

Domain	Objektif kontrol	Kontrol keamanan	Temuan	Rekomendasi
		A.9.4.4 : Penggunaan program utilitas dengan hak istimewa	Program utilitas pada aplikasi SIMAK seperti fitur untuk menghapus, mengimport dan mengeksport data masih belum diawasi, beberapa kasus pernah terjadi terkait menu utilitas, seperti terhapusnya data, ini tentu saja sangat berbahaya, karena integritas data dapat terancam oleh kases yang tidak sah. Pendokumentasian, pembatasan dan pematauan mutlak dilakukan untuk memantau program utilitas pada aplikasi SIMAK.	UPTTIK harus memantau setiap program atau menu utilitias pada aplikasi SIMAK, peraturan dan dokumentasi terkait penentuan pemegang hak program utilitas harus dibuat, setiap program utilitas harus dibatasi hak aksesnya.
		A.9.4.5 : Kontrol akses ke kode sumber program	Kode sumber atau source code aplikasi SIMAK diamankan oleh hak akses, hanya orang yang mempunyai akses tertentu saja yang dapat mengakses kode sumber tersebut, pengguna harus menggunakan VPN untuk dapat mengakses kode sumber tersebut, namun belum ada kebijakan atau peraturan yng mengatur terkait siapa saja yang dapat mengakses kode sumber tersebut.	UPTTIK harus membuat peraturan secara tertulis terkait akses terhadap kode sumber atau source code, pendokumentasian perlu dilakukan terhadap aktivitas akses terhadap source code, karyawan yang berhak mengakses source code harus ditentukan, harus dibuat dokumen yang ditandatangani oleh karywan terkait mengamankan kerahasiaan dan keamanan source code

Tabel lampiran C. 10 Temuan dan Rekomendasi (Lanjutan)

Domain	Objektif kontrol	Kontrol keamanan	Temuan	Rekomendasi
A.11 : Keamanan fisik dan lingkungan	A.11.1 : Area aman	A.11.1.1 : Pembatas keamanan fisik	Perimeter atau pembatas keamanan fisik telah ada untuk mengamankan server aplikasi SIMAK, pebatas keamanan tersebut berupa kunci pintu sidik jari, tidak hanya satu tetapi terdapat 3 lapis perimeter keamanan, yang pertama adalah kunci pintu biasa, yang kedua dan ketiga adalah kunci pintu yang hanya bisa diakses menggunakan sidik jari pengguna yang telah terdaftar, ruangan server aplikasi SIMAK juga di kelilingi oleh dinding beton, namun ada beberap bagian dari ruangan server yang berbatasan langsung denagan ruangan lain yang hanya di batasi oleh dinding kaca biasa, tentu ini bisa jadi ancaman keamanan karena bisa saja akses tidak sah melalui jalur tersebut.	Perimeter pembatas fisik harus di*review* secara berkala, seluruh pembatas keamaman fisk harus berdasarkan standar ruangan server.

Tabel lampiran C. 11 Temuan dan Rekomendasi (Lanjutan)

Domain	Objektif kontrol	Kontrol keamanan	Temuan	Rekomendasi
		A.11.1.2 : Kontrol entri fisik	Secure area atau area aman terdapat pada UPTTIK, yang pertama adalah bagian luar, tengah dan dalam, pada ruangan dalam (ruang server) juga sudah di rancang sebagai ruangan aman untuk bekerja, petugas yang bertugas memelihara server aplikasi SIMAK dapat bekerja secara aman, baik dari gangguan bencana alam ataupun dari gangguan lain seperti aliran listrik dan lain sebagainya.	Area aman harus dir*eview* secara berkala untuk memastikan keamanan pegawai atau karyawan yang sedang bekerja, untuk akses ke ruang server dan secure area harus menggunakan ID pengenal, harus dibuat peraturan terdokumentasi terkait kebijakan dan peraturan mengenai kontrol entri fisik
		A.11.1.3 : Tedapat keamanan ruangan dan fasilitas kantor	Ruangan kantor dan ruangan server aplikasi UPTTIK pada perancangannya tidak mengacu pada rancangan bangunan yang di peruntukan untuk server, namun meski begitu keamanan standar seperti dinding pembatas, dinding beton dan kunci keamanan telah terpasang untuk mengamankan ruangan UPTTIK dan ruangan server dari gangguan,baik gangguan alam maupun gangguan akses jahat.	Ruangan kantor sudah sesuai standar, semua aea terlindungi adai gangguan akses tidak sah atau pun gangguan alam, ruangan server aplikasi SIMAK belum mengadopsi suatu standar ruangan server, untuk jangka pendek harus segera di *review* dan dilakukan penyesuaina ruangan.

Tabel lampiran C. 12 Temuan dan Rekomendasi (Lanjutan)

Domain	Objektif kontrol	Kontrol keamanan	Temuan	Rekomendasi
		A.11.1.4 : Melindungi dari ancaman eksternal dan lingkungan	Ruangan server aplikasi SIMAK tidak dirancang sebagai ruangan server, ada beberapa kelemahan yang dapat menjadi ancaman bagi keamanan data atau pengguna, seperti kabel jaringan dan kabel listrik tidak dipisahkan jalurnya, tidak ada pendingan yang khusus di peruntukan untuk ruangan server, jalur kabel tidak melalui jalur nawah lantai, dan beberapa kelemahan lainnya, kelemahan kelemhan tersebut dapat menjadi ancaman, baik ancaman alam ataupun ancaman yang berasal dari gangguan manusia.	Dindingkaca yang menyekat ruang server denagan ruang rapat pada satu bagian harus segera di*review* dan dilakukan penyesuain.
		A.11.1.5 : Bekerja di tempat yang aman	Terdapat area aman untuk bekerja pada UPTTIK, seluruh ruangan pada UPTTIK disesuaikan agar dapat menjadi ruangan yang aman untuk bekerja, juga ruangan server aplkasi SIMAK telah disesuaikan untuk menjadi secure area, namun meski begitu secure area belum berdasarkan suatu standar keamanan tertentu.	Area bekerja harus di*review* secara berkala untuk memastikan keamanan pekerja, ruangan *server* harus di*review* untuk selanjutnya disesuaikan mengikuti standar ruangan *server*, seperti penempatan kabel listrik dan jaringan agar supaya pekerja bekerja lebih aman.

Tabel lampiran C. 13 Temuan dan Rekomendasi (Lanjutan)

Domain	Objektif kontrol	Kontrol keamanan	Temuan	Rekomendasi
		A.11.1.6 : Area pengiriman dan pemuatan	Area pengiriman dan pemuatan barang dikelola dan dikendalikan oleh bagian khusus, namun bukan oleh karyawan dari UPTTIK, seluruh barang yang di tujukan eke UPTTIK diperiksa dan dicatat oleh bagian yang bertugas mengelola barang. Mekanisme pemeriksaan barang tidak berdasarkan pada standar keamanan, dan hanya berupa pengecekan biasa terhadap kesesuaian barang.	Area ppengiriman dan pemuatan sudah terpisan, area pemuatan harus dilakukan *review* secara rutin, pengawasan terkait barang yang masuk aharus dilakukan oleh orang yang berwenang, harus dialakukan pendokumentasian terkait barang yang masuk dan keluar dari UPTTIK.
	A.11.2 : Peralatan	A.11.2.1 : Penempatan dan perlindungan peralatan	Terdapat pengidentifikasian lokasi tempat barang akan di tempatkan, pemilihan lokasi berdasarkan peniliaian keamanan dan ancaman, ancaman berupa ancaman internal maupun ancaman eksternal. Contohnya kertika pemilihan lokasi jalur kabel jaringan, pemilihan lokasi rack UPS telah mempertimbangkan potensi ancamn yang akan muncul, baik ancaman manusia ataupun alam.	Penempatan peralatan pada server SIAMAK harus *direview* secara rutin, harus dlakukan pendokumentasian terkait dengan pemilihan dan penempatan peralatan pada suatu lokasi.

Tabel lampiran C. 14 Temuan dan Rekomendasi (Lanjutan)

Domain	Objektif kontrol	Kontrol keamanan	Temuan	Rekomendasi
		A.11.2.2 : Utilitas pendukung	Server aplikasi SIMAK telah menggunakan UPS sebagai daya cadangan ketika aliran listrik mati, UPS dapat mem-backup daya selama kurang lebih 2 jam, namun hal itu bukan berdasarkan suatu panduan keamanan.	Server apliksi SIMAK telah menggunakan UPS sebagai backup dayanya, harus dilakukan pengukuran terkait ketahanan UPS dalam membackup server SIMAK, generator genset perlu dikaji sebagai opsi backup cadangan untuk daya tahan backup energi yang lebih lama dan lebih besar.
		A.11.2.3 : Keamanan kabel	Penilaian keamanan kabel jaringan dan kabel listrik telah dilakukan ketika memilih lokasi penempatannya, pemilihan lokasi bertujuan agar kabel lsitrikk dan jaringan jauh atau terhindar dari gangguan, namun meski demikian pemilihan lokasi hanya berdasarkan asumsi, buka merujuk pada satu panduan keamanan.	Lokasi kabel harus *direview* secara rutin, pemilihan lokasi kabel listrik dan jarinagan harus secara terpisah, pada rruangan server SIKAK, kabel listrik dan jaringan harus menggunakan jalur bawah lantai.
		A.11.2.4 : Perawatan peralatan	Perawatan terhadap alat - alat server kerap kali dilakukan, tidak ada jadwal rutin yang mengharuskan atau mengatur kapan peralatan server aplikasi SIMAK harus dirawat, perawatan dilakun apabila ditemukan perubahan suatu kondisi yang menyebabkan terganggunaya kinerja sever..	Harus dibaut SOP (standar operational procedure) terkait perawatan server aplikasi SIMAK secara terjadwal dan rutin, perawatan harus dilakukan oleh orang yang berkompeten, perawatan server aplikasi SIMAK harus terdokumentasi, perwatan server harus *direview* secara berkala.

Tabel lampiran C. 15 Temuan dan Rekomendasi (Lanjutan)

Domain	Objektif kontrol	Kontrol keamanan	Temuan	Rekomendasi
		A.11.2.5 : Penghapusan aset	Proses penghapusan perangkat dilakukan oleh bagian yang bertugas mengelola barang, UPTTIK sebagai pemakai hanya memastikan bahawa barang yang masukan ke dalam daftar aset yang akan dihapus benar - benar sudah tidak dapat digunakan kembali dan memastikan tidak ada lagi data sensitif pada barang yang akan di hapus.	Penghapusan asset harus diatur dalam peratuaran tertulis, terkait mekanisme penghapusan data didalamnya, harus dilakukan verifikasi terkait apakah ada data sensitif atau tidak pada asset yang akan dihapus atau dibuang.
		A.11.2.6 : Keamanan peralatan dan aset di luar lokasi	Kebiajakan terkait keamanan perangkat yang ditempatkan diluar lokasi telah ada, namu hanya berupa intrukksi dari pimpinan UPTTIK secara lisan dan belum terdokumentasi.	Harus dibuat peraturan tertulis terkait emenjaga keamanan asset yang berada diluar lokasi.
		A.11.2.7 : Pembuangan yang aman atau penggunaan kembali peralatan	Barang yang akan di buang atau di gunakan lagi diperiksa oleh masing - masing penanggungjawab atas barang tersebut, pemegang barang harus benar-benar memastikan barang yang dikelolanya ketika akan di buang atau tidak di gunnakan lagi benar - benar kosong atau tidak mengandung data sensitif, juga barang yang akan di b uang tidak lagi memiliki lisensi software didalamnya.	UPTTIK harus membuat prosedur tertulis terkait barang yang akan dibuang atau digunakan kembali, misal penggunaan atau pembuangan hardisk, flash drive, dan penyimpanan lainnya yang dianggap mengandung data yang dapat dimanfaat kan oleh orang yang tidak bertanggungjawab.

Tabel lampiran C. 16 Temuan dan Rekomendasi (Lanjutan)

Domain	Objektif kontrol	Kontrol keamanan	Temuan	Rekomendasi
		A.11.2.8 : Peralatan pengguna tanpa pengawasan	Kebijakan terkait perlindungan peralatan yang dipakai oleh karyawan di komunikasikan secara lisan oleh pimpinan kepada seluruh karyawan, pimpinan memberikan arahan terhadap pengguna untuk mengamankan perangkat yang ia gunakan, pengkentikan sesi aktif, mel-logout aplikasi, hal ini bertujan supaya tidak ada ases ilegal oleh orang yang tidak bertanggugjawab terhadap aplikasi SIMAK.	UPTTIK harus membuat kebijakan atau peraturan secara tertlis terkait pengawasan asset pengguna yang tanpa pengawasan, mengunci laptop atau komputer untuk menjaga kerahasiaan dan menghindari akses tidak sah, menutup session aktif yang terhubung pada server atau aplikasi SIMAK.
		A.11.2.9 : Kebijakan Clear desk and clear screen	Pimpian menhimbau kepada seluruh karyawan untu kerbiasa dengan kebijakan clear desk dan clear screen , hal ini dimaksudkan supaya tidak ada data data sensitif yang tertinggal pada meja yang bisa saja dimanfaatkan oleh orang yang tidak bertanggungjawab, data dapat berupa catatan password dan kode akses lainnya, misalkan kode akses untuk mengakses server aplikasi SIMAK.	UPTTIK harus membuat dokumentasi tertulis terkait kebijakan yang mengatur clear screen, clear desk, karayawan harus diberi wpenyuluhan terkait denganpentingnya menerapkan prosedur clear screen, clear desk, catatan - catatan kecil yang berisi data - data harus dibersihkan dan dihancurkan dari atas wmeja kerja, hal ini dilakukan untuk menjaga kerahasiaan data agar tidak digunakan oelh orang yang tidak bertanggungjawab.

LAMPIRAN D

Tabel lampiran D. 1 Responden 1

A.5	Kebijakan Keamanan Informasi				
A.5.1	Arahan manajemen untuk keamanan informasi		Pertanyaan	Ya	Tidak
A.5.1.1	Kebijakan untuk keamanan informasi	1	Apakah terdapat kebijakan keamanan informasi terkait pengelolaan informasi?	✓	
		2	Apakah kebijakan keamanan Informasi tersebut disetujui oleh manajemen dan pimpinan?	✓	
		3	Apakah kebijakan dikomunikasikan secara baik kepada karyawan?		✓
		4	Apakah kebikakan dibuat sesuai dengan tujuan organisasi?	✓	
		5	Apakah kebijakan dapat disesuaikan apabila ditemukan perubahan suatu kondisi?		✓
A.5.1.2	*Review* kebijakan untuk keamanan informasi	1	Apakah dilakukan peninjauan terhadap kebijakan keamanan informasi?	✓	
		2	Apakah peninjauan dilakunan secara berkala?		✓
		3	Apakah peninjauan melibatkan manajemen dan pimpinan?		✓
		4	Apakah *review* dilakukan berdasarkan kebutuhan oraganisasi?	✓	
		5	Apakah dilakukan *review* terhadap kebijakan apabila ditemukan perubahan situasi?	✓	
A.6	Keamanan Informasi Organisasi		Pertanyaan	Ya	Tidak
A.6.1	Internal Organisasi				
A.6.1.1	Peran dan tanggung jawab keamanan informasi	1	Apakah tanggung jawab terkait perlindungan perangkat pribadi, untuk melaksanakan proses keamanan, diidentifikasi, dan dikomunikasikan kepada pihak terkait?	✓	
		2	Apakah peran dan tanggungjawab telah sesuai dengan keahlian masing - masing karyawan?	✓	

Tabel lampiran D. 2 Responden 1 (Lanjutan)

		3	Apakah terdapat dokumentasi terkait pelaksanaan tugas dan tanggungjawab dalam menjaga informasi organisasi?		✓□
		4	Apakah peran dan tanggungjawab karyawan sudah sesuai dengan tujuan organisasi?	✓□	
		5	Apakah dilakuakan *review* terkait peran dan tanggungjawab karayawan dalam menjaga keamanan informasi organisasi?		✓□
A.6.1.2	Pemisahan tugas	1	Apakah tugas dan bidang tanggung jawab dipisahkan, untuk mengurangi peluang modifikasi yang tidak sah atau penyalahgunaan informasi, atau layanan?	✓□	
		2	Apakah pemisahan tugas sudah sesuai dengan keahlian masing - masing karyawan?	✓□	
		3	Apakah pemisahan tugas sudah sesuai dengan kebijakan organisasi?		✓□
		4	Apakah pemisahan tugas, bidang dan tanggungajawab sudah sesuai dengan tujuan atau visi misi organisasi?		✓□
		5	Apakah pemisahan tugas, bidang dan tanggungjawab *direview* apabila ditemukan perubahan suatu kondisi?	✓□	
A.6.1.3	Kontak dengan pihak berwenang	1	Apakah terdapat prosedur yang mendokumentasikan kapan, dan oleh siapa, kontak dengan otoritas terkait akan dilakukan?		✓□
		2	Apakah kontak dengan otoritas terkait disetujui oleh manajemen?	✓□	
		3	Apakah terdapat proses yang merinci bagaimana dan kapan kontak perlu dilakukan?		✓□
		4	Apakah terdapat proses untuk kontak rutin dan berbagi pengetahuan?		✓□
		5	Apakah kontak dengan pihak terkait dilakukan secara rutin?		✓□
A.6.1.4	Kontak dengan kelompok minat khusus	1	Apakah terdapat pihak yang berwenang untuk mengaktifkan keanggotaan?	✓□	
		2	Apakah pengaktifan keanggotaan sudah dilakukan oleh pihak yang sesuai?	✓□	

Tabel lampiran D. 3 Responden 1 (Lanjutan)

		3	Apakah pengaktifan keanggotaan sudah diketahui oleh manajemen dan pimpinan?		✓□
		4	Apakah pengaktifan keanggotaan sesuai atau sejalan dengan tujuan organiasasi?		✓□
		5	Apakah dilakukan *review* terkait pengaktifan keanggotaan apabila ditemukan perubahan suatu kondisi?		✓□
A.6.1.5	Keamanan informasi dalam manajemen proyek	1	Apakah seluruh proyek sudah melalui beberapa penilaian keamanan informasi?	✓□	
		2	Apakah penilaian terkait keamanan informasi sudah mengacu pada suatu standar?		✓□
		3	Apakah penilaian keamanan informasi terdokumentasi?		✓□
		4	Apakah penilaian keamanan informasi sesuai dengan tujuan organisasi?	✓□	
		5	Apakah penilaian keamanan informasi pada suatu proyek dilakukan secara rutin sesuai tahapan proyek?	✓□	
A.6.2	Perangkat Seluler dan *Teleworking*		Pertanyaan	Ya	Tidak
A.6.2.1	Kebijakan perangkat seluler	1	Apakah terdapat kebijakan terkait perangkat seluler?	✓□	
		2	Apakah kebijakan terkait perangkat seluer terdokumentasi?		✓□
		3	Apakah terdapat kebijakan yang mendokumentasikan dan menangani risiko dari penggunaan perangkat seluler (penggunaan hotspot ilegal)?		✓□
		4	Apakah kebijakan terkait perangkat selular sesuai dengan tujuan organisasi?	✓□	
		5	Apakah kebijakan terkait perangkat seluler *direview* apabila ditemukan perubahan pada suatu kondisi?		✓□
A.6.2.2	*Teleworking*	1	Apakah terdapat kebijakan untuk *teleworking* (kerja diluar kantor) misalnya kerja dari rumah (WFH)?	✓□	
		2	Apakah *teleworking* mendapat persetujuan manajemen?	✓□	

Tabel lampiran D. 4 Responden 1 (Lanjutan)

		3	Apakah terdapat mekanisme atau proses yang ditetapkan bagi pekerja jarak jauh untuk mendapatkan akses (terhadap layanan/sistem)?	✓	
		4	Apakah karyawan yang akan melakukan WFH diberi pengarahan terkait perlindungan perangkat yang mereka gunakan?		✓
		5	Apakah dilakukan *review* terkait kebijakan WFH apabila ditemukan perubahan suatu kondisi?		✓
A.9	Kontrol akses		Pertanyaan	Ya	Tidak
A.9.1	Persyaratan bisnis untuk kontrol akses				
A.9.1.1	Kebijakan kontrol akses	1	Apakah terdapat kebijakan kontrol akses?	✓	
		2	Apakah terdapat kebijakan terkait kontrol akses berdasarkan kebutuhan proses bisnis?	✓	
		3	Apakah kebijakan terkait kontrol akses dikomunikasikan dengan baik dengan manajemen?		✓
		4	Apakah kebijakan terkait kontrol akses sudah sesuai dengan tujuan organisasi?		✓
		5	Apakah kebijakan terkait kontrol akses di*review* apabila ditemukan perubahan pada suatu kondisi?		✓
A.9.1.2	Akses ke jaringan dan layanan jaringan	1	Apakah terdapat kontrol untuk memastikan pengguna hanya memiliki akses ke jaringan khusus yang diperlukan untuk tugas mereka?	✓	
		2	Apakah kontrol pengguna pada suatu jaringan sudah disetujui manajemen?	✓	
		3	Apakah layanan jaringan sudah dikomunikasikan secara baik kepada pihak terkait?		✓
		4	Apakah layanan jaringan yang didapatkan pengguna sudah mengacu pada suatu standar?		✓
		5	Apakah dilakukan perubahan layanan terkait akses jaringan apabila ditemukan perubahan suatu kondisi?		✓
A.9.2	Manajemen akses pengguna		Pertanyaan	Ya	Tidak

Tabel lampiran D. 5 Responden 1 (Lanjutan)

A.9.2.1	Pendaftaran pengguna dan pencabutan pendaftaran	1	Apakah terdapat proses pendaftaran akses untuk pengguna secara formal?	✓□	
		2	Apakah proses pendaftaran akses untuk pengguna sudah disetujui oleh manajemen?	✓□	
		3	Apakah proses pendaftaran akses untuk pengguna sudah terdokumentasi?		✓□
		4	Apakah pemberian akses untuk pengguna sudah sesuai dengan tujuan organisasi?		✓□
		5	Apakah akses unntuk pengguna *direview* apabila ditemukan perubahan suatu kondisi?	✓□	
A.9.2.2	Penyediaan akses pengguna	1	Apakah terdapat proses penyediaan akses bagi pengguna untuk menetapkan hak akses semua jenis dan layanan?	✓□	
		2	Apakah proses penyediaan akases bagi pengguna sudah disetujui oleh manajemen?	✓□	
		3	Apakah penyediaan akses untuk pengguna sudah terdokumentasi?		✓□
		4	Apakah penyediaan akses untuk pengguna sudah sesuai dengan tujuan organisasi?	✓□	
		5	Apakah dilakukan *review* terkait penyediaan akses untuk pengguna apabila ditemukan perubahan suatu kondisi?	✓□	
A.9.2.3	Pengelolaan hak akses istimewa	1	Apakah akun dengan akses istimewa (admin dan super admin) dikelola dan dikontrol secara terpisah?	✓□	
		2	Apakah pengelolaan akses super admin dan super admin mengacu pada suatu standar keamanan?		✓□
		3	Apakah pengelolaan akun admin dan super admin sudah terdokumentasi?		✓□
		4	Apakah pengelolaan akun admin dan super admin sudah sesuai dengan tujuan organisasi?	✓□	
		5	Apakah dilakukan *review* terkait pengelolaan akun admin dan superadmin apabila ditemukan perubahan suatu kondisi?		✓□

Tabel lampiran D. 6 Responden 1 (Lanjutan)

A.9.2.4	Pengelolaan informasi otentikasi rahasia pengguna	1	Apakah terdapat proses manajemen secara formal untuk mengontrol informasi rahasia?	✓	
		2	Apakah pengelolaan informasi rahasia pengguna sudah mengacu pada suatu standar keamanan?		✓
		3	Apakah mekanisme pengelolaan data rahasia pengguna telah dikomunikasikan secara baik kepada seluruh karyawan terkait?		✓
		4	Apakah proses pengelolaan data rahasia pengguna diketahui oleh manajemen?		✓
		5	Apak dialakukan *review* terkait pengelolaan data rahasia pengguna apabila ditemukan perubahan kondisi?	✓	
A.9.2.5	*Review* hak akses pengguna	1	Apakah terdapat proses bagi pemilik perangkat untuk meninjau hak akses ke perangkat mereka secara teratur?	✓	
		2	Apakah proses tinjauan ini diverifikasi?		✓
		3	Apakah proses *review* terdokumentasi?		✓
		4	Apakah proses *review* terkait hak akses pengguna mendapat persetujuan manajemen?	✓	
		5	Apakah proses *review* sudah sesuai dengan tujuan organisasi?	✓	
A.9.2.6	Penghapusan atau penyesuaian hak akses	1	Apakah terdapat mekanisme dan proses untuk memastikan hak akses pengguna dihapus saat pemutusan hubungan kerja, atau saat perubahan peran?	✓	
		2	Apakah proses untuk penghapusan hak akses sudah diketahui oleh manajemen?	✓	
		3	Apakah proses penghapusan kah akses terdokumentasi?		✓
		4	Apakah proses penghapusan dan penyesuaian hak akses sudah sesuai dengan tujuan oraganisasi?	✓	
		5	Apakah dilakukan *review* terkait proses penghapusan dan penyesuaian hak akses apabila ditemukan perubahan suatu kondisi?	✓	
A.9.3	Tanggung jawab pengguna		Pertanyaan	Ya	Tidak

Tabel lampiran D. 7 Responden 1 (Lanjutan)

A.9.3.1	Penggunaan informasi otentikasi rahasia	1	Apakah terdapat dokumen kebijakan yang mencakup praktik organisasi tentang bagaimana informasi otentikasi rahasia harus ditangani?		✓
		2	Apakah dokumen tersebut dikomunikasikan kepada semua pengguna?		✓
		3	Apakah dokumen tersebut mengacu pada sebuah standar keamanan?		✓
		4	Apakah penanganan informasi rahasia sudah sesuai denagan tujuan organisasi?		✓
		5	Apakah dilakukan *review* terhadap dokumen yang berisi tentang penanganan informasi rahasia pengguna apabila ditemukan perubahan suatu kondisi?		✓
A.9.4	Kontrol akses sistem dan aplikasi		Pertanyaan	Ya	Tidak
A.9.4.1	Pembatasan akses informasi	1	Apakah akses terhadap informasi dan fungsi sistem aplikasi dibatasi sesuai dengan kebijakan kontrol akses?	✓	
		2	Apakah pembatasan akses terhadap informasi dan fungsi aplikasi disetujui oleh manajemen?		✓
		3	Apakah pembatasan akses terhadap inforamasi dan fungsi aplikasi sudah dikomunikasikan kepada seluruh karyawan?		✓
		4	Apakah pembatasan akses terhadap inforamasi dan fungsi aplikasi sesuai dengan tujuan organisasi?	✓	
		5	Apakah dilakuakan *review* terkait pembatasan informasi dan fungsi apalikasi apabila ditemukan perubahan suatu kondisi?	✓	
A.9.4.2	Amankan prosedur log-on	1	Apakah akses dikontrol oleh prosedur log-on yang aman?	✓	
		2	Apaakah prosesudh log-on sudah mengacu pada suatu standar keamanan?		✓
		3	Apakah terdapat mekanisme yang mendokumentasikan prosedur log-on?		✓
		4	apakah prosedur log-on dirancang agar terhindar dari gangguan pihak jahat?	✓	

Tabel lampiran D. 8 Responden 1 (Lanjutan)

		5	Apakah terdapat mekanisme *review* terkait keamanan prosedur log-on apabila dietemukan isu atau perubahan suatu kondisi?	✓	
A.9.4.3	Sistem manajemen kata sandi	1	Apakah sistem kata sandi bersifat interaktif?	✓	
		2	Apakah diperlukan kata sandi yang rumit?		✓
		3	Apakah manajemen kata sandi sudah mengacu pada suatu standar keamanan?		✓
		4	Apakah terdapat kewajiban untuk mengganti kata sandi secara rutin?		✓
		5	Apakah manajemen pengelolaan kata sandi *direview* apabila ditemukan perubahan suatu kondisi?	✓	
A.9.4.4	Penggunaan program utilitas dengan hak istimewa	1	Apakah program utilitas hak istimewa dibatasi dan dipantau?	✓	
		2	Apakah penggunaan program utilitas dengan hak istimewa sudah disetujui oleh manajemen?		✓
		3	Apakah penggunaan program utilitas dengan hak istimewa sudah terdokumentasi?		✓
		4	Apakah penggunaan program utilitas dengan hak istimewa sudah sesuai dengan kebijakan dan tujuan organisasi?	✓	
		5	Apakah dilakuna *review* terkait penggunaan program utilitas dengan hak akses istimewa apabila ditemukan perubahan suatu kondisi?		✓
A.9.4.5	Kontrol akses ke kode sumber program	1	Apakah akses terhadap kode sumber *(Source Code)* sistem dilindungi oleh kontrol akses?	✓	
		2	Apakah perlindungan terhadap source code disetujui oleh manajemen?	✓	
		3	Apakah perlindungan terhadap source code di komunikasikan terhadap seluruh karyawan terkait?		✓
		4	Apakah perlindungan terhadap source code sudah sesuai dengan tujuan dan arahan organisasi?	✓	

Tabel lampiran D. 9 Responden 1 (Lanjutan)

		5	Apakah dilakukan *review* terkait perlindungan source code apabila ditemukan perubahan suatu kondisi?		✓□
A.11	Keamanan fisik dan lingkungan		Pertanyaan	Ya	Tidak
A.11.1	Area aman				
A.11.1.1	Perimeter (pembatas) keamanan fisik	1	Apakah terdapat perimeter (pembatas) keamanan khusus?	✓□	
		2	Apakah area informasi sensitif atau kritis dipisahkan dan dikontrol dengan baik?	✓□	
		3	Apakah pembatas keamanan fisik sudah sesuai berdasarkan standar keamanan?		✓□
		4	Apakah pembatas keamanan fisik dirancang untuk perlindungan terhadap ancaman kejahatan?		✓□
		5	Apakah pembatas fisik dievaluasti apabila ditemukan perubahan kondisi?	✓□	
A.11.1.2	Kontrol entri fisik	1	Apakah area aman *(secure area)* memiliki sistem kontrol masuk yang sesuai untuk memastikan hanya personel yang berwenang yang memiliki akses?	✓□	
		2	Apakah secure area telah mengikuti standar keamanan?		✓□
		3	Apakah kontrol entri sudah sesuai dengan kebijakan organisaisi?	✓□	
		4	Apakahpersonel yang dapat masuk ke secure area sudah sesuai dengan kebijakan organisasi?	✓□	
		5	Apakah kontrol entri terhadap secure area *direview* apabila ditemukan perubahan terhadap suatu kondisi?		✓□
A.11.1.3	Mengamankan kantor, kamar, dan fasilitas	1	Apakah ruangan kantor dan fasilitas lain telah dirancang dan dikonfigurasi dengan mempertimbangkan keamanan?		✓□
		2	Apakah terdapat proses untuk menjaga keamanan (misalnya mengunci, membersihkan meja, dll.)?	✓□	
		3	Apak terkait keamanan ruangan sudah dikomunikasikan dengan baik kepada karayawan?		✓□
		4	apakah ruangan kantor sudah sesuai dengan suatu standar?		✓□

Tabel lampiran D. 10 Responden 1 (Lanjutan)

		5	Apakah dilakuna *review* terhadap keamanan kantor atau ruangan apabila ditemukan perubahan suatu kondisi?	✓	
A.11.1.4	Melindungi dari ancaman eksternal dan lingkungan	1	Apakah perlindungan fisik untuk mencegah bencana alam, serangan jahat atau kecelakaan telah dirancang?		✓
		2	Apakah perlindungan fisik terkait ancaman bencana alam atau serangan jahat sudah disetujui oleh manajemen?	✓	
		3	Apakah perlindungan fisik sudah terdukomentasi?		✓
		4	Apakah perlindungan fisik terkait ancaman bencana alam dan pihak jahat sudah sesuai standar keamanan?		✓
		5	Apakah dilakukan *review* terkait rancanagan perlindungan fisik apabila ditemukan perubahan suatu kondisi?	✓	
A.11.1.5	Bekerja di tempat yang aman	1	Apakah terdapat area aman *(Secure Area)?*	✓	
		2	Apakah s*ecure area* memiliki kebijakan dan proses yang sesuai?	✓	
		3	Apakah kebijakan dan proses dilakukan dan dipantau?	✓	
		4	Apakah secure area sudah distujui organisasi?	✓	
		5	Apakah dilakukan *review* terkait secure area apabila ditemukan perubahan pada suatu kondisi?		✓
A.11.1.6	Area pengiriman dan pemuatan	1	Apakah terdapat area pengiriman / pemuatan yang terpisah?	✓	
		2	Apakah akses ke area pengiriman/pemuatan dikendalikan?	✓	
		3	Apakah akses area pemuatan diisolasi dari fasilitas pemrosesan informasi?		✓
		4	Apakah lokasi pemuatan sudah sesuai dengan standar kemanan?		✓
		5	Apakah area pengiriman dan pemuatan *direview* apabila ditemukan perubahan suatu kondisi?		✓
A.11.2	Peralatan		Pertanyaan	Ya	Tidak
A.11.2.1	Penempatan dan perlindungan peralatan	1	Apakah bahaya lingkungan diidentifikasi dan dipertimbangkan ketika lokasi peralatan dipilih?	✓	

Tabel lampiran D. 11 Responden 1 (Lanjutan)

		2	Apakah risiko akses yang tidak sah telah dipertimbangkan saat menentukan lokasi peralatan?		✓□
		3	Apakah penempatan peralatan sudah terdokumentasi?	✓□	
		4	Apakah penempatan peralatan sudah seuasuai dengan kebutuhan organisasi?	✓□	
		5	Apaha dilakukan *review* terkait penempatan dan perlindungan peralatan apabila ditemukan perubahan suatu kondisi?		✓□
A.11.2.2	Utilitas pendukung	1	Apakah terdapat UPS atau generator cadangan?	✓□	
		2	Apakah sistem UPS sudah diuji dalam skala waktu yang sesuai?		✓□
		3	Apakah UPS yangdigunakan sudah berdasarkan suatu standar?		✓□
		4	Apakah penggunaan UPS sudah berdasarkan kebutuhan organisasi?	✓□	
		5	Apakah terdapat mekanisme *review* terkait penggunaan UPS apabila ditemukan perubahan suatu kondisi?	✓□	
A.11.2.3	Keamanan kabel	1	Apakah penilaian risiko telah dilakukan atas lokasi kabel listrik dan kabel telekomunikasi atau jaringan?	✓□	
		2	Apakah kabel listrik dan jaringan ditempatkan supaya terlindung dari gangguan, intersepsi, atau kerusakan?	✓□	
		3	Apakah penempatan kabel lstrik dan jaringan sudah terdokumentasi?		✓□
		4	Apakah penentuan tempat kabel listrik dan jaringan sudah berdasarkan penilaian ancaman bencana alam dan ancaman pihak jahat?		✓□
		5	Apakah dilakukan *review* terkait penempatan posisi kabel dan ajaringan apabila ditemukan perubahan suatu kondisi?	✓□	
A.11.2.4	Perawatan peralatan	1	Apakah terdapat jadwal perawatan peralatan yang ketat?		✓□
		2	Apaakah perawatan peralatan diketahui oleh manajemen?	✓□	
		3	Apakah perawatan peralatan terdokumentasi?		✓□

Tabel lampiran D. 12 Responden 1 (Lanjutan)

		4	Apakah perawatan peralatan keamanan sudah sesuai dengan standar kemanan?		✓□
		5	Apakah dilakukan *review* terkait terawatan keamanan apabila ditemukan perubahan suatu kondisi?	✓□	
A.11.2.5	Penghapusan perangkat	1	Apakah terdapat proses yang mengontrol bagaimana perangkat dihapus dari daftar perangkat?	✓□	
		2	Apakah proses kontol penghapusan perangkat dilakukan?		✓□
		3	Apakah pemeriksaan langsung terhadap proses penghapusan perangkat dilakukan?	✓□	
		4	Apakah pengahapusan perangkat sudah disetujui oleh manajemen dan pimpinan?		✓□
		5	Apakah dilakukan *review* terkait penghapusan perangkat dari daftar peranghat apabila ditemukan perubahan suatu kondisi?	✓□	
A.11.2.6	Keamanan peralatan dan perangkat di luar lokasi	1	Apakah terdapat kebijakan yang mengatur keamanan perangkat di luar lokasi?		✓□
		2	Apakah kebijakan perlindungan perangkat diluar lokasi (kantor) dikomunikasikan secara luas?		✓□
		3	Apakah penempatan perlatan diluar lokasi terdokumentasi?		✓□
		4	Apakah penempatan perlatan diluar lokasi sudah memperhitungkan bahaya keamanan bencana alam atau ancaman prilaku jahat?	✓□	
		5	Apakah dilakukan *review* terkait perlindungan peralatan diluar lokasi?	✓□	
A.11.2.7	Pembuangan yang aman atau penggunaan kembali peralatan	1	Apakah terdapat kebijakan yang mengatur bagaimana perangkat informasi dapat digunakan kembali?		✓□
		2	Apakah mekanisme pengelolaan data, diverifikasi dengan benar sebelum digunakan kembali / dibuang?	✓□	
		3	Apakah kebijakan penggunaan atau pembuanagan data sudah dikomunikasikan secara baik kepada karyawan?		✓□

Tabel lampiran D. 13 Responden 1 (Lanjutan)

		4	Apakah pembuangan atau penggunaan kembali peralatan sudah berdasarkan pertimbangan keamanan?		✓□
		5	Apakah terdapat mekanisme *review* terkait penggunaan atau pembuangan apabila ditemukan perubahan suatu kondisi?	✓□	
A.11.2.8	Peralatan pengguna tanpa pengawasan	1	Apakah organisasi memiliki kebijakan tentang bagaimana peralatan yang tidak dijaga harus dilindungi?		✓□
		2	Apakah kontrol teknis diterapkan untuk mengamankan peralatan yang secara tidak sengaja ditinggalkan?		✓□
		3	Apakah terdapat pendokumentasian terhadap barang - barang yang tidak sengaja ditinggalkan?		✓□
		4	Apakah kebijakan terkait perlindungan perlatan yang tidak sengaja ditinggalkan sudah diketahui pimpinan dan manajemen?		✓□
		5	Apakah dilakukan *review* terkait kebijakan perlindungan barang yang tdaik sengaja ditinggalkan?	✓□	
A.11.2.9	Kebijakan *Clear desk and clear screen*	1	Apakah terdapat kebijakan *clear desk /clear screen?*	✓□	
		2	Apakah kebijakan clear desk dan clear screen diberlakukan dengan baik?		✓□
		3	Apakah kebijakan terkait clear screen dan clear desk sudah dikomunikasikan dengan baik dengan karyawan?		✓□
		4	Apakah kebijakan clear screen dan clear desk sudah sesuai dengan kebutuhan organisasi?	✓□	
		5	Apakah dilakukan *review* terhadap kebijakan clear screen dan clear desk apabila ditemukan perubahan suatu kondisi?	✓□	

Tabel lampiran D. 14 Responden 2

A.5	Kebijakan Keamanan Informasi		Pertanyaan	Ya	Tidak
A.5.1	Arahan manajemen untuk keamanan informasi				
A.5.1.1	Kebijakan untuk keamanan informasi	1	Apakah terdapat kebijakan keamanan informasi terkait pengelolaan informasi?	✓	
		2	Apakah kebijakan keamanan Informasi tersebut disetujui oleh manajemen dan pimpinan?	✓	
		3	Apakah kebijakan dikomunikasikan secara baik kepada karyawan?		✓
		4	Apakah kebikakan dibuat sesuai dengan tujuan organisasi?	✓	
		5	Apakah kebijakan dapat disesuaikan apabila ditemukan perubahan suatu kondisi?	✓	
A.5.1.2	*Review* kebijakan untuk keamanan informasi	1	Apakah dilakukan peninjauan terhadap kebijakan keamanan informasi?	✓	
		2	Apakah peninjauan dilakunan secara berkala?		✓
		3	Apakah peninjauan melibatkan manajemen dan pimpinan?		✓
		4	Apakah *review* dilakukan berdasarkan kebutuhan oraganisasi?	✓	
		5	Apakah dilakukan *review* terhadap kebijakan apabila ditemukan perubahan situasi?		✓
A.6	Keamanan Informasi Organisasi		Pertanyaan	Ya	Tidak
A.6.1	Internal Organisasi				
A.6.1.1	Peran dan tanggung jawab keamanan informasi	1	Apakah tanggung jawab terkait perlindungan perangkat pribadi, untuk melaksanakan proses keamanan, diidentifikasi, dan dikomunikasikan kepada pihak terkait?		✓
		2	Apakah peran dan tanggungjawab telah sesuai dengan keahlian masing - masing karyawan?	✓	
		3	Apakah terdapat dokumentasi terkait pelaksanaan tugas dan tanggungjawab dalam menjaga informasi organisasi?		✓
		4	Apakah peran dan tanggungjawab karyawan sudah sesuai dengan tujuan organisasi?	✓	

Tabel lampiran D. 15 Responden 2 (Lanjutan)

		5	Apakah dilakuakan *review* terkait peran dan tanggungjawab karayawan dalam menjaga keamanan informasi organisasi?	✓	
A.6.1.2	Pemisahan tugas	1	Apakah tugas dan bidang tanggung jawab dipisahkan, untuk mengurangi peluang modifikasi yang tidak sah atau penyalahgunaan informasi, atau layanan?	✓	
		2	Apakah pemisahan tugas sudah sesuai dengan keahlian masing - masing karyawan?		✓
		3	Apakah pemisahan tugas sudah sesuai dengan kebijakan organisasi?	✓	
		4	Apakah pemisahan tugas, bidang dan tanggungajawab sudah sesuai dengan tujuan atau visi misi organisasi?	✓	
		5	Apakah pemisahan tugas, bidang dan tanggungjawab di*review* apabila ditemukan perubahan suatu kondisi?	✓	
A.6.1.3	Kontak dengan pihak berwenang	1	Apakah terdapat prosedur yang mendokumentasikan kapan, dan oleh siapa, kontak dengan otoritas terkait akan dilakukan?		✓
		2	Apakah kontak dengan otoritas terkait disetujui oleh manajemen?	✓	
		3	Apakah terdapat proses yang merinci bagaimana dan kapan kontak perlu dilakukan?		✓
		4	Apakah terdapat proses untuk kontak rutin dan berbagi pengetahuan?		✓
		5	Apakah kontak dengan pihak terkait dilakukan secara rutin?		✓
A.6.1.4	Kontak dengan kelompok minat khusus	1	Apakah terdapat pihak yang berwenang untuk mengaktifkan keanggotaan?	✓	
		2	Apakah pengaktifan keanggotaan sudah dilakukan oleh pihak yang sesuai?	✓	
		3	Apakah pengaktifan keanggotaan sudah diketahui oleh manajemen dan pimpinan?		✓
		4	Apakah pengaktifan keanggotaan sesuai atau sejalan dengan tujuan organiasasi?	✓	
		5	Apakah dilakukan *review* terkait pengaktifan keanggotaan apabila ditemukan perubahan suatu kondisi?	✓	

Tabel lampiran D. 16 Responden 2 (Lanjutan)

A.6.1.5	Keamanan informasi dalam manajemen proyek	1	Apakah seluruh proyek sudah melalui beberapa penilaian keamanan informasi?		✓□
		2	Apakah penilaian terkait keamanan informasi sudah mengacu pada suatu standar?		✓□
		3	Apakah penilaian keamanan informasi terdokumentasi?		✓□
		4	Apakah penilaian keamanan informasi sesuai dengan tujuan organisasi?	✓□	
		5	Apakah penilaian keamanan informasi pada suatu proyek dilakukan secara rutin sesuai tahapan proyek?	✓□	
A.6.2	Perangkat Seluler dan *Teleworking*		Pertanyaan	Ya	Tidak
A.6.2.1	Kebijakan perangkat seluler	1	Apakah terdapat kebijakan terkait perangkat seluler?	✓□	
		2	Apakah kebijakan terkait perangkat selular mendapat persetujuan manajemen?		✓□
		3	Apakah terdapat kebijakan yang mendokumentasikan dan menangani risiko dari penggunaan perangkat seluler (penggunaan hotspot ilegal)?	✓□	
		4	Apakah kebijakan terkait perangkat selular sesuai dengan tujuan organisasi?	✓□	
		5	Apakah kebijakan terkait perangkat seluler di*review* apabila ditemukan perubahan pada suatu kondisi?	✓□	
A.6.2.2	*Teleworking*	1	Apakah terdapat kebijakan untuk *teleworking* (kerja diluar kantor) misalnya kerja dari rumah (WFH)?	✓□	
		2	Apakah *teleworking* mendapat persetujuan manajemen?	✓□	
		3	Apakah terdapat mekanisme atau proses yang ditetapkan bagi pekerja jarak jauh untuk mendapatkan akses (terhadap layanan/sistem)?	✓□	
		4	Apakah karyawan yang akan melakukan WFH diberi pengarahan terkait perlindungan perangkat yang mereka gunakan?		✓□
		5	Apakah dilakukan *review* terkait kebijakan WFH apabila ditemukan perubahan suatu kondisi?		✓□
A.9	Kontrol akses		Pertanyaan	Ya	Tidak

Tabel lampiran D. 17 Responden 2 (Lanjutan)

A.9.1	Persyaratan bisnis untuk kontrol akses				

A.9.1.1	Kebijakan kontrol akses	1	Apakah terdapat kebijakan kontrol akses?	✓	
		2	Apakah terdapat kebijakan terkait kontrol akses berdasarkan kebutuhan proses bisnis?		✓
		3	Apakah kebijakan terkait kontrol akses dikomunikasikan dengan baik dengan manajemen?		✓
		4	Apakah kebijakan terkait kontrol akses sudah sesuai dengan tujuan organisasi?	✓	
		5	Apakah kebijakan terkait kontrol akses di *review* apabila ditemukan perubahan pada suatu kondisi?	✓	
A.9.1.2	Akses ke jaringan dan layanan jaringan	1	Apakah terdapat kontrol untuk memastikan pengguna hanya memiliki akses ke jaringan khusus yang diperlukan untuk tugas mereka	✓	
		2	Apakah kontrol pengguna pada suatu jaringan sudah disetujui manajemen?	✓	
		3	Apakah layanan jaringan sudah dikomunikasikan secara baik kepada pihak terkait?		✓
		4	Apakah layanan jaringan yang didapatkan pengguna sudah mengacu pada suatu standar?		✓
		5	Apakah dilakukan perubahan layanan terkait akses jaringan apabila ditemukan perubahan suatu kondisi?	✓	
A.9.2	Manajemen akses pengguna		Pertanyaan	Ya	Tidak
A.9.2.1	Pendaftaran pengguna dan pencabutan pendaftaran	1	Apakah terdapat proses pendaftaran akses untuk pengguna secara formal?		✓
		2	Apakah proses pendaftaran akses untuk pengguna sudah disetujui oleh manajemen?	✓	
		3	Apakah proses pendaftaran akses untuk pengguna sudah terdokumentasi?		✓
		4	Apakah pemberian akses untuk pengguna sudah sesuai dengan tujuan organisasi?	✓	

Tabel lampiran D. 18 Responden 2 (Lanjutan)

		5	Apakah akses unntuk pengguna di*review* apabila ditemukan perubahan suatu kondisi?		✓□
A.9.2.2	Penyediaan akses pengguna	1	Apakah terdapat proses penyediaan akses bagi pengguna untuk menetapkan hak akses semua jenis dan layanan?	✓□	
		2	Apakah proses penyediaan akases bagi pengguna sudah disetujui oleh manajemen?	✓□	
		3	Apakah penyediaan akses untuk pengguna sudah terdokumentasi?		✓□
		4	Apakah penyediaan akses untuk pengguna sudah sesuai dengan tujuan organisasi?	✓□	
		5	Apakah dilakukan *review* terkait penyediaan akses untuk pengguna apabila ditemukan perubahan suatu kondisi?		✓□
A.9.2.3	Pengelolaan hak akses istimewa	1	Apakah akun dengan akses istimewa (admin dan super admin) dikelola dan dikontrol secara terpisah?		✓□
		2	Apakah pengelolaan akses super admin dan super admin mengacu pada suatu standar keamanan?		✓□
		3	Apakah pengelolaan akun admin dan super admin sudah terdokumentasi?		✓□
		4	Apakah pengelolaan akun admin dan super admin sudah sesuai dengan tujuan organisasi?	✓□	
		5	Apakah dilakukan *review* terkait pengelolaan akun admin dan superadmin apabila ditemukan perubahan suatu kondisi?	✓□	
A.9.2.4	Pengelolaan informasi otentikasi rahasia pengguna	1	Apakah terdapat proses manajemen secara formal untuk mengontrol informasi rahasia?	✓□	
		2	Apakah pengelolaan informasi rahasia pengguna sudah mengacu pada suatu standar keamanan?		✓□
		3	Apakah mekanisme pengelolaan data rahasia pengguna telah dikomunikasikan secara baik kepada seluruh karyawan terkait?		✓□
		4	Apakah proses pengelolaan data rahasia pengguna diketahui oleh manajemen?	✓□	

Tabel lampiran D. 19 Responden 2 (Lanjutan)

		5	Apak dialakukan *review* terkait pengelolaan data rahasia pengguna apabila ditemukan perubahan kondisi?		✓□
A.9.2.5	*Review* hak akses pengguna	1	Apakah terdapat proses bagi pemilik perangkat untuk meninjau hak akses ke perangkat mereka secara teratur?		✓□
		2	Apakah proses tinjauan ini diverifikasi?		✓□
		3	Apakah proses *review* terdokumentasi?		✓□
		4	Apakah proses *review* terkait hak akses pengguna mendapat persetujuan manajemen?		✓□
		5	Apakah proses *review* sudah sesuai dengan tujuan organisasi?		✓□
A.9.2.6	Penghapusan atau penyesuaian hak akses	1	Apakah terdapat mekanisme dan proses untuk memastikan hak akses pengguna dihapus saat pemutusan hubungan kerja, atau saat perubahan peran?	✓□	
		2	Apakah proses untuk penghapusan hak akses sudah diketahui oleh manajemen?		✓□
		3	Apakah proses penghapusan kah akses terdokumentasi?		✓□
		4	Apakah proses penghapusan dan penyesuaian hak akses sudah sesuai dengan tujuan oraganisasi?	✓□	
		5	Apakah dilakukan *review* terkait proses penghapusan dan penyesuaian hak akses apabila ditemukan perubahan suatu kondisi?	✓□	
A.9.3	Tanggung jawab pengguna		Pertanyaan	Ya	Tidak
A.9.3.1	Penggunaan informasi otentikasi rahasia	1	Apakah terdapat dokumen kebijakan yang mencakup praktik organisasi tentang bagaimana informasi otentikasi rahasia harus ditangani?		✓□
		2	Dokumen tersebut dikomunikasikan kepada semua pengguna		✓□
		3	Apakah dokumen tersebut mengacu pada sebuah standar keamanan?		✓□
		4	Apakah penanganan informasi rahasia sudah sesuai denagan tujuan organisasi?		✓□
		5	Apakah dilakukan *review* terhadap dokumen yang berisi tentang penanganan informasi rahasia pengguna apabila ditemukan perubahan suatu kondisi?		✓□

Tabel lampiran D. 20 Responden 2 (Lanjutan)

A.9.4	Kontrol akses sistem dan aplikasi		Pertanyaan	Ya	Tidak

A.9.4.1	Pembatasan akses informasi	1	Apakah akses terhadap informasi dan fungsi sistem aplikasi dibatasi sesuai dengan kebijakan kontrol akses?	✓	
		2	Apakah pembatasan akses terhadap informasi dan fungsi aplikasi disetujui oleh manajemen?		✓
		3	Apakah pembatasan akses terhadap inforamasi dan fungsi aplikasi sudah dikomunikasikan kepada seluruh karyawan?		✓
		4	Apakah pembatasan akses terhadap inforamasi dan fungsi aplikasi sesuai dengan tujuan organisasi?		✓
		5	Apakah dilakuakan *review* terkait pembatasan informasi dan fungsi apalikasi apabila ditemukan perubahan suatu kondisi?	✓	
A.9.4.2	Amankan prosedur *log-on*	1	Apakah akses dikontrol oleh prosedur log-on yang aman?	✓	
		2	Apakah prosedur log-on sudah mengacu pada suatu standar keamanan?		✓
		3	Apakah terdapat mekanisme yang mendokumentasikan prosedur log-on?		✓
		4	Apakah prosedur log-on dirancang agar terhindar dari gangguan pihak jahat?	✓	
		5	Apakah terdapat mekanisme *review* terkait keamanan prosedur log-on apabila dietemukan isu atau perubahan suatu kondisi?	✓	
A.9.4.3	Sistem manajemen kata sandi	1	Apakah sistem kata sandi bersifat interaktif?		✓
		2	Apakah diperlukan kata sandi yang rumit?		✓
		3	Apakah manajemen kata sandi sudah mengacu pada suatu standar keamanan?	✓	
		4	Apakah terdapat kewajiban untuk mengganti kata sandi secara rutin?		✓
		5	Apakah manajemen pengelolaan kata sandi di*review* apabila ditemukan perubahan suatu kondisi?	✓	
A.9.4.4	Penggunaan program utilitas dengan hak istimewa	1	Apakah program utilitas hak istimewa dibatasi dan dipantau?		✓

Tabel lampiran D. 21 Responden 2 (Lanjutan)

		2	Apakah penggunaan program utilitas dengan hak istimewa sudah disetujui oleh manajemen?	✓	

		3	Apakah penggunaan program utilitas dengan hak istimewa sudah terdokumentasi?		✓□
		4	Apakah penggunaan program utilitas dengan hak istimewa sudah sesuai dengan kebijakan dan tujuan organisasi?		✓□
		5	Apakah dilakuna review terkait penggunaan program utilitas dengan hak akses istimewa apabila ditemukan perubahan suatu kondisi?	✓□	
A.9.4.5	Kontrol akses ke kode sumber program	1	Apakah akses terhadap kode sumber *(Source Code)* sistem dilindungi oleh kontrol akses?	✓□	
		2	Apakah perlindungan terhadap source code disetujui oleh manajemen?	✓□	
		3	Apakah perlindungan terhadap source code di komunikasikan terhadap seluruh karyawan terkait?		✓□
		4	Apakah perlindungan terhadap source code sudah sesuai dengan tujuan dan arahan organisasi?	✓□	
		5	Apakah dilakukan review terkait perlindungan source code apabila ditemukan perubahan suatu kondisi?	✓□	
A.11	Keamanan fisik dan lingkungan		Pertanyaan	Ya	Tidak
A.11.1	Area aman				
A.11.1.1	Perimeter (pembatas) keamanan fisik	1	Apakah terdapat perimeter (pembatas) keamanan khusus?	✓□	
		2	Apakah area informasi sensitif atau kritis dipisahkan dan dikontrol dengan baik?	✓□	
		3	Apakah pembatas keamanan fisik sudah sesuai berdasarkan standar keamanan?		✓□
		4	Apakah pembatas keamanan fisik dirancang untuk perlindungan terhadap ancaman kejahatan?	✓□	
		5	Apakah pembatas fisik dievaluasti apabila ditemukan perubahan kondisi?	✓□	

Tabel lampiran D. 22 Responden 2 (Lanjutan)

A.11.1.2	Kontrol entri fisik	1	Apakah area aman *(secure area)* memiliki sistem kontrol masuk yang sesuai untuk memastikan hanya personel yang berwenang yang memiliki akses?	✓	
		2	Apakah secure area telah mengikuti standar keamanan?		✓
		3	Apakah kontrol entri sudah sesuai dengan kebijakan organisaisi?	✓	
		4	Apakahpersonel yang dapat masuk ke secure area sudah sesuai dengan kebijakan organisasi?		✓
		5	Apakah kontrol entri terhadap secure area direview apabila ditemukan perubahan terhadap suatu kondisi?	✓	
A.11.1.3	Mengamankan kantor, kamar, dan fasilitas	1	Apakah ruangan kantor dan fasilitas lain telah dirancang dan dikonfigurasi dengan mempertimbangkan keamanan?	✓	
		2	Apakah terdapat proses untuk menjaga keamanan (misalnya mengunci, membersihkan meja, dll.)?	✓	
		3	Apak terkait keamanan ruangan sudah dikomunikasikan dengan baik kepada karayawan?		✓
		4	apakah ruangan kantor sudah sesuai dengan suatu standar?	✓	
		5	Apakah dilakuna review terhadap keamanan kantor atau ruangan apabila ditemukan perubahan suatu kondisi?	✓	
A.11.1.4	Melindungi dari ancaman eksternal dan lingkungan	1	Apakah perlindungan fisik untuk mencegah bencana alam, serangan jahat atau kecelakaan telah dirancang?		✓
		2	Apakah perlindungan fisik terkait ancaman bencana alam atau serangan jahat sudah disetujui oleh manajemen?	✓	
		3	Apakah perlindungan fisik sudah terdukomentasi?		✓
		4	Apakah perlindungan fisik terkait ancaman bencana alam dan pihak jahat sudah sesuai standar keamanan?		✓
		5	Apakah dilakukan review terkait rancanagan perlindungan fisik apabila ditemukan perubahan suatu kondisi?	✓	
A.11.1.5	Bekerja di tempat yang aman	1	Apakah terdapat area aman *(Secure Area)?*	✓	
		2	Apakah s*ecure area* memiliki kebijakan dan proses yang sesuai?	✓	

Tabel lampiran D. 23 Responden 2 (Lanjutan)

		3	Apakah kebijakan dan proses dilakukan dan dipantau?		✓

		4	Apakah secure area sudah distujui organisasi?	✓	
		5	Apakah dilakukan review terkait secure area apabila ditemukan perubahan pada suatu kondisi?	✓	
A.11.1.6	Area pengiriman dan pemuatan	1	Apakah terdapat area pengiriman / pemuatan yang terpisah?	✓	
		2	Apakah akses ke area pengiriman/pemuatan dikendalikan?	✓	
		3	Apakah akses area pemuatan diisolasi dari fasilitas pemrosesan informasi?		✓
		4	Apakah lokasi pemuatan sudah sesuai dengan standar kemanan?		✓
		5	Apakah area pengiriman dan pemuatan direview apabila ditemukan perubahan suatu kondisi?	✓	
A.11.2	Peralatan		Pertanyaan	Ya	Tidak
A.11.2.1	Penempatan dan perlindungan peralatan	1	Apakah bahaya lingkungan diidentifikasi dan dipertimbangkan ketika lokasi peralatan dipilih?		✓
		2	Apakah risiko akses yang tidak sah telah dipertimbangkan saat menentukan lokasi peralatan?	✓	
		3	Apakah penempatan peralatan sudah terdokumentasi?	✓	
		4	Apakah penempatan peralatan sudah seuasuai dengan kebutuhan organisasi?	✓	
		5	Apakah dilakukan review terkait penempatan dan perlindungan peralatan apabila ditemukan perubahan suatu kondisi?	✓	
A.11.2.2	Utilitas pendukung	1	Apakah terdapat UPS atau generator cadangan?	✓	
		2	Apakah sistem UPS sudah diuji dalam skala waktu yang sesuai?	✓	
		3	Apakah UPS yang digunakan sudah berdasarkan suatu standar?	✓	
		4	Apakah penggunaan UPS sudah berdasarkan kebutuhan organisasi?	✓	
		5	Apakah terdapat mekanisme review terkait penggunaan UPS apabila ditemukan perubahan suatu kondisi?	✓	

Tabel lampiran D. 24 Responden 2 (Lanjutan)

A.11.2.3	Keamanan kabel	1	Apakah penilaian risiko telah dilakukan atas lokasi kabel listrik dan kabel telekomunikasi atau jaringan?	✓	

		2	Apakah kabel listrik dan jaringan ditempatkan supaya terlindung dari gangguan, intersepsi, atau kerusakan?	✓	
		3	Apakah penempatan kabel lstrik dan jaringan sudah terdokumentasi?		✓
		4	Apakah penentuan tempat kabel listrik dan jaringan sudah berdasarkan penilaian ancaman bencana alam dan ancaman pihak jahat?	✓	
		5	Apakah dilakukan review terkait penempatan posisi kabel dan ajaringan apabila ditemukan perubahan suatu kondisi?		✓
A.11.2.4	Perawatan peralatan	1	Apakah terdapat jadwal perawatan peralatan yang ketat?		✓
		2	Apaakah perawatan peralatan diketahui oleh manajemen?	✓	
		3	Apakah perawatan peralatan terdokumentasi?	✓	
		4	Apakah perawatan peralatan keamanan sudah sesuai dengan standar kemanan?		✓
		5	Apakah dilakukan review terkait terawatan keamanan apabila ditemukan perubahan suatu kondisi?	✓	
A.11.2.5	Penghapusan perangkat	1	Apakah terdapat proses yang mengontrol bagaimana perangkat dihapus dari daftar perangkat?	✓	
		2	Apakah proses kontol penghapusan perangkat dilakukan?	✓	
		3	Apakah pemeriksaan langsung terhadap proses penghapusan perangkat dilakukan?	✓	
		4	Apakah pengahapusan perangkat sudah disetujui oleh manajemen dan pimpinan?		✓
		5	Apakah dilakukan review terkait penghapusan perangkat dari daftar peranghat apabila ditemukan perubahan suatu kondisi?	✓	
A.11.2.6	Keamanan peralatan dan perangkat di luar lokasi	1	Apakah terdapat kebijakan yang mengatur keamanan perangkat di luar lokasi?	✓	
		2	Apakah kebijakan perlindungan perangkat diluar lokasi (kantor) dikomunikasikan secara luas?	✓	

Tabel lampiran D. 25 Responden 2 (Lanjutan)

		3	Apakah penempatan perlatan diluar lokasi terdokumentasi?	✓	
		4	Apakah penempatan perlatan diluar lokasi sudah memperhitungkan bahaya keamanan bencana alam atau ancaman prilaku jahat?		✓

		5	Apakah dilakukan review terkait perlindungan peralatan diluar lokasi?	✓	
A.11.2.7	Pembuangan yang aman atau penggunaan kembali peralatan	1	Apakah terdapat kebijakan yang mengatur bagaimana perangkat informasi dapat digunakan kembali?	✓	
		2	Apakah mekanisme pengelolaan data, diverifikasi dengan benar sebelum digunakan kembali / dibuang?	✓	
		3	Apakah kebijakan penggunaan atau pembuanagan data sudah dikomunikasikan secara baik kepada karyawan?		✓
		4	Apakah pembuangan atau penggunaan kembali peralatan sudah berdasarkan pertimbangan keamanan?		✓
		5	Apakah terdapat mekanisme review terkait penggunaan atau pembuangan apabila ditemukan perubahan suatu kondisi?	✓	
A.11.2.8	Peralatan pengguna tanpa pengawasan	1	Apakah organisasi memiliki kebijakan tentang bagaimana peralatan yang tidak dijaga harus dilindungi?		✓
		2	Apakah kontrol teknis diterapkan untuk mengamankan peralatan yang secara tidak sengaja ditinggalkan?		✓
		3	Apakah terdapat pendokumentasian terhadap barang - barang yang tidak sengaja ditinggalkan?	✓	
		4	Apakah terdapat kebijakan terkait perlindungan perlatan yang tidak sengaja ditinggalkan sudah diketahui pimpinan dan manajemen?		✓
		5	Apakah dilakukan review terkait kebijakan perlindungan barang yang tdaik sengaja ditinggalkan?	✓	
A.11.2.9	Kebijakan *Clear desk and clear screen*	1	Apakah terdapat kebijakan *clear desk /clear screen?*	✓	
		2	Apakah kebijakan clear desk dan clear screen diberlakukan dengan baik?	✓	
		3	Apakah kebijakan terkait clear screen dan clear desk sudah dikomunikasikan dengan baik dengan karyawan?	✓	

Tabel lampiran D. 26 Responden 2 (Lanjutan)

		4	Apakah kebijakan clear screen dan clear desk sudah sesuai dengan kebutuhan organisasi?		✓
		5	Apakah dilakukan review terhadap kebijakan clear screen dan clear desk apabila ditemukan perubahan suatu kondisi?	✓	

Tabel lampiran D. 27 Responden 3

A.5	Kebijakan Keamanan Informasi		Pertanyaan	Ya	Tidak
A.5.1	Arahan manajemen untuk keamanan informasi				
A.5.1.1	Kebijakan untuk keamanan informasi	1	Apakah terdapat kebijakan keamanan informasi terkait pengelolaan informasi?	✓	
		2	Apakah kebijakan keamanan Informasi tersebut disetujui oleh manajemen dan pimpinan?	✓	
		3	Apakah kebijakan dikomunikasikan secara baik kepada karyawan?		✓
		4	Apakah kebijakan dibuat sesuai dengan tujuan organisasi?	✓	
		5	Apakah kebijakan dapat disesuaikan apabila ditemukan perubahan suatu kondisi?	✓	
A.5.1.2	Review kebijakan untuk keamanan informasi	1	Apakah dilakukan peninjauan terhadap kebijakan keamanan informasi?		✓
		2	Apakah peninjauan dilakunan secara berkala?		✓
		3	Apakah peninjauan melibatkan manajemen dan pimpinan?		✓
		4	Apakah review dilakukan berdasarkan kebutuhan oraganisasi?	✓	
		5	Apakah dilakukan review terhadap kebijakan apabila ditemukan perubahan situasi?	✓	
A.6	Keamanan Informasi Organisasi		Pertanyaan	Ya	Tidak
A.6.1	Internal Organisasi				

Tabel lampiran D. 28 Responden 2 (Lanjutan)

A.6.1.1	Peran dan tanggung jawab keamanan informasi	1	Apakah tanggung jawab terkait perlindungan perangkat pribadi, untuk melaksanakan proses keamanan, diidentifikasi, dan dikomunikasikan kepada pihak terkait?	✓	
		2	Apakah peran dan tanggungjawab telah sesuai dengan keahlian masing - masing karyawan?	✓	

		3	Apakah terdapat dokumentasi terkait pelaksanaan tugas dan tanggungjawab dalam menjaga informasi organisasi?		✓
		4	Apakah peran dan tanggungjawab karyawan sudah sesuai dengan tujuan organisasi?		✓
		5	Apakah dilakuakan review terkait peran dan tanggungjawab karayawan dalam menjaga keamanan informasi organisasi?	✓	
A.6.1.2	Pemisahan tugas	1	Apakah tugas dan bidang tanggung jawab dipisahkan, untuk mengurangi peluang modifikasi yang tidak sah atau penyalahgunaan informasi, atau layanan?		✓
		2	Apakah pemisahan tugas sudah sesuai dengan keahlian masing - masing karyawan?	✓	
		3	Apakah pemisahan tugas sudah sesuai dengan kebijakan organisasi?		✓
		4	Apakah pemisahan tugas, bidang dan tanggungajawab sudah sesuai dengan tujuan atau visi misi organisasi?		✓
		5	Apakah pemisahan tugas, bidang dan tanggungjawab direview apabila ditemukan perubahan suatu kondisi?	✓	
A.6.1.3	Kontak dengan pihak berwenang	1	Apakah terdapat prosedur yang mendokumentasikan kapan, dan oleh siapa, kontak dengan otoritas terkait akan dilakukan?		✓
		2	Apakah kontak dengan otoritas terkait disetujui oleh manajemen?	✓	
		3	Apakah terdapat proses yang merinci bagaimana dan kapan kontak perlu dilakukan?	✓	
		4	Apakah terdapat proses untuk kontak rutin dan berbagi pengetahuan?	✓	
		5	Apakah kontak dengan pihak terkait dilakukan secara rutin?		✓

Tabel lampiran D. 29 Responden 2 (Lanjutan)

A.6.1.4	Kontak dengan kelompok minat khusus	1	Apakah terdapat pihak yang berwenang untuk mengaktifkan keanggotaan?	✓	
		2	Apakah pengaktifan keanggotaan sudah dilakukan oleh pihak yang sesuai?		✓

		3	Apakah pengaktifan keanggotaan sudah diketahui oleh manajemen dan pimpinan?		✓□
		4	Apakah pengaktifan keanggotaan sesuai atau sejalan dengan tujuan organiasasi?	✓□	
		5	Apakah dilakukan review terkait pengaktifan keanggotaan apabila ditemukan perubahan suatu kondisi?		✓□
A.6.1.5	Keamanan informasi dalam manajemen proyek	1	Apakah seluruh proyek sudah melalui beberapa penilaian keamanan informasi?		✓□
		2	Apakah penilaian terkait keamanan informasi sudah mengacu pada suatu standar?		✓□
		3	Apakah penilaian keamanan informasi terdokumentasi?		✓□
		4	Apakah penilaian keamanan informasi sesuai dengan tujuan organisasi?	✓□	
		5	Apakah penilaian keamanan informasi pada suatu proyek dilakukan secara rutin sesuai tahapan proyek?	✓□	
A.6.2	Perangkat Seluler dan *Teleworking*		Pertanyaan	Ya	Tidak
A.6.2.1	Kebijakan perangkat seluler	1	Apakah terdapat kebijakan terkait perangkat seluler?	✓□	
		2	Apakah kebijakan terkait perangkat selular mendapat persetujuan manajemen?	✓□	
		3	Apakah terdapat kebijakan yang mendokumentasikan dan menangani risiko dari penggunaan perangkat seluler (penggunaan hotspot ilegal)?		✓□
		4	Apakah kebijakan terkait perangkat selular sesuai dengan tujuan organisasi?		✓□
		5	Apakah kebijakan terkait perangkat seluler direview apabila ditemukan perubahan pada suatu kondisi?	✓□	

Tabel lampiran D. 30 Responden 2 (Lanjutan)

A.6.2.2	*Teleworking*	1	Apakah terdapat kebijakan untuk *teleworking* (kerja diluar kantor) misalnya kerja dari rumah (WFH)?		✓□
		2	Apakah *teleworking* mendapat persetujuan manajemen?	✓□	

		3	Apakah terdapat mekanisme atau proses yang ditetapkan bagi pekerja jarak jauh untuk mendapatkan akses (terhadap layanan/sistem)?		✓□
		4	Apakah karyawan yang akan melakukan WFH diberi pengarahan terkait perlindungan perangkat yang mereka gunakan?		✓□
		5	Apakah dilakukan review terkait kebijakan WFH apabila ditemukan perubahan suatu kondisi?	✓□	
A.9	Kontrol akses		Pertanyaan	Ya	Tidak
A.9.1	Persyaratan bisnis untuk kontrol akses				
A.9.1.1	Kebijakan kontrol akses	1	Apakah terdapat kebijakan kontrol akses?	✓□	
		2	Apakah terdapat kebijakan terkait kontrol akses berdasarkan kebutuhan proses bisnis?		✓□
		3	Apakah kebijakan terkait kontrol akses dikomunikasikan dengan baik dengan manajemen?	✓□	
		4	Apakah kebijakan terkait kontrol akses sudah sesuai dengan tujuan organisasi?		✓□
		5	Apakah kebijakan terkait kontrol akses di review apabila ditemukan perubahan pada suatu kondisi?	✓□	
A.9.1.2	Akses ke jaringan dan layanan jaringan	1	Apakah terdapat kontrol untuk memastikan pengguna hanya memiliki akses ke jaringan khusus yang diperlukan untuk tugas mereka?		✓□
		2	Apakah kontrol pengguna pada suatu jaringan sudah disetujui manajemen?	✓□	
		3	Apakah layanan jaringan sudah dikomunikasikan secara baik kepada pihak terkait?		✓□
		4	Apakah layanan jaringan yang didapatkan pengguna sudah mengacu pada suatu standar?		✓□

Tabel lampiran D. 31 Responden 2 (Lanjutan)

		5	Apakah dilakukan perubahan layanan terkait akses jaringan apabila ditemukan perubahan suatu kondisi?	✓□	
A.9.2	Manajemen akses pengguna		Pertanyaan	Ya	Tidak

A.9.2.1	Pendaftaran pengguna dan pencabutan pendaftaran	1	Apakah terdapat proses pendaftaran akses untuk pengguna secara formal?	✓□	
		2	Apakah proses pendaftaran akses untuk pengguna sudah disetujui oleh manajemen?	✓□	
		3	Apakah proses pendaftaran akses untuk pengguna sudah terdokumentasi?	✓□	
		4	Apakah pemberian akses untuk pengguna sudah sesuai dengan tujuan organisasi?		✓□
		5	Apakah akses unntuk pengguna direview apabila ditemukan perubahan suatu kondisi?	✓□	
A.9.2.2	Penyediaan akses pengguna	1	Apakah terdapat proses penyediaan akses bagi pengguna untuk menetapkan hak akses semua jenis dan layanan?	✓□	
		2	Apakah proses penyediaan akases bagi pengguna sudah disetujui oleh manajemen?	✓□	
		3	Apakah penyediaan akses untuk pengguna sudah terdokumentasi?	✓□	
		4	Apakah penyediaan akses untuk pengguna sudah sesuai dengan tujuan organisasi?		✓□
		5	Apakah dilakukan review terkait penyediaan akses untuk pengguna apabila ditemukan perubahan suatu kondisi?		✓□
A.9.2.3	Pengelolaan hak akses istimewa	1	Apakah akun dengan akses istimewa (admin dan super admin) dikelola dan dikontrol secara terpisah?		✓□
		2	Apakah pengelolaan akses super admin dan super admin mengacu pada suatu standar keamanan?		✓□
		3	Apakah pengelolaan akun admin dan super admin sudah terdokumentasi?		✓□

Tabel lampiran D. 32 Responden 2 (Lanjutan)

		4	Apakah pengelolaan akun admin dan super admin sudah sesuai dengan tujuan organisasi?	✓□	

		5	Apakah dilakukan review terkait pengelolaan akun admin dan superadmin apabila ditemukan perubahan suatu kondisi?	✓□	
A.9.2.4	Pengelolaan informasi otentikasi rahasia pengguna	1	Apakah terdapat proses manajemen secara formal untuk mengontrol informasi rahasia?	✓□	
		2	Apakah pengelolaan informasi rahasia pengguna sudah mengacu pada suatu standar keamanan?		✓□
		3	Apakah mekanisme pengelolaan data rahasia pengguna telah dikomunikasikan secara baik kepada seluruh karyawan terkait?		✓□
		4	Apakah proses pengelolaan data rahasia pengguna diketahui oleh manajemen?	✓□	
		5	Apak dialakukan review terkait pengelolaan data rahasia pengguna apabila ditemukan perubahan kondisi?	✓□	
A.9.2.5	Review hak akses pengguna	1	Apakah terdapat proses bagi pemilik perangkat untuk meninjau hak akses ke perangkat mereka secara teratur?	✓□	
		2	Apakah proses tinjauan ini diverifikasi?		✓□
		3	Apakah proses review terdokumentasi?		✓□
		4	Apakah proses review terkait hak akses pengguna mendapat persetujuan manajemen?	✓□	
		5	Apakah proses review sudah sesuai dengan tujuan organisasi?	✓□	
A.9.2.6	Penghapusan atau penyesuaian hak akses	1	Apakah terdapat mekanisme dan proses untuk memastikan hak akses pengguna dihapus saat pemutusan hubungan kerja, atau saat perubahan peran?		✓□
		2	Apakah proses untuk penghapusan hak akses sudah diketahui oleh manajemen?		✓□
		3	Apakah proses penghapusan kah akses terdokumentasi?		✓□
		4	Apakah proses penghapusan dan penyesuaian hak akses sudah sesuai dengan tujuan oraganisasi?	✓□	

Tabel lampiran D. 33 Responden 2 (Lanjutan)

		5	Apakah dilakukan review terkait proses penghapusan dan penyesuaian hak akses apabila ditemukan perubahan suatu kondisi?	✓□	
A.9.3	Tanggung jawab pengguna		Pertanyaan	Ya	Tidak

A.9.3.1	Penggunaan informasi otentikasi rahasia	1	Apakah terdapat dokumen kebijakan yang mencakup praktik organisasi tentang bagaimana informasi otentikasi rahasia harus ditangani?		✓
		2	Dokumen tersebut dikomunikasikan kepada semua pengguna		✓
		3	Apakah dokumen tersebut mengacu pada sebuah standar keamanan?		✓
		4	Apakah penanganan informasi rahasia sudah sesuai denagan tujuan organisasi?	✓	
		5	Apakah dilakukan review terhadap dokumen yang berisi tentang penanganan informasi rahasia pengguna apabila ditemukan perubahan suatu kondisi?	✓	
A.9.4	Kontrol akses sistem dan aplikasi		Pertanyaan	Ya	Tidak
A.9.4.1	Pembatasan akses informasi	1	Apakah akses terhadap informasi dan fungsi sistem aplikasi dibatasi sesuai dengan kebijakan kontrol akses?	✓	
		2	Apakah pembatasan akses terhadap informasi dan fungsi aplikasi disetujui oleh manajemen?		✓
		3	Apakah pembatasan akses terhadap inforamasi dan fungsi aplikasi sudah dikomunikasikan kepada seluruh karyawan?		✓
		4	Apakah pembatasan akses terhadap inforamasi dan fungsi aplikasi sesuai dengan tujuan organisasi?	✓	
		5	Apakah dilakuakan review terkait pembatasan informasi dan fungsi apalikasi apabila ditemukan perubahan suatu kondisi?	✓	
A.9.4.2	Amankan prosedur log-on	1	Apakah akses dikontrol oleh prosedur log-on yang aman?	✓	
		2	Apakah prosedurlog-on sudah mengacu pada suatu standar keamanan?	✓	
		3	Apakah terdapat mekanisme yang mendokumentasikan prosedur log-on?		✓
		4	apakah prosedur log-on dirancang agar terhindar dari gangguan pihak jahat?	✓	

Tabel lampiran D. 34 Responden 2 (Lanjutan)

		5	Apakah terdapat mekanisme review terkait keamanan prosedur log-on apabila dietemukan isu atau perubahan suatu kondisi?	✓	
A.9.4.3	Sistem manajemen kata sandi	1	Apakah sistem kata sandi bersifat interaktif?		✓
		2	Apakah diperlukan kata sandi yang rumit?		✓

		3	Apakah manajemen kata sandi sudah mengacu pada suatu standar keamanan?	✓	
		4	Apakah terdapat kewajiban untuk mengganti kata sandi secara rutin?		✓
		5	Apakah manajemen pengelolaan kata sandi direview apabila ditemukan perubahan suatu kondisi?	✓	
A.9.4.4	Penggunaan program utilitas dengan hak istimewa	1	Apakah program utilitas hak istimewa dibatasi dan dipantau?		✓
		2	Apakah penggunaan program utilitas dengan hak istimewa sudah disetujui oleh manajemen?	✓	
		3	Apakah penggunaan program utilitas dengan hak istimewa sudah terdokumentasi?		✓
		4	Apakah penggunaan program utilitas dengan hak istimewa sudah sesuai dengan kebijakan dan tujuan organisasi?		✓
		5	Apakah dilakuna review terkait penggunaan program utilitas dengan hak akses istimewa apabila ditemukan perubahan suatu kondisi?	✓	
A.9.4.5	Kontrol akses ke kode sumber program	1	Apakah akses terhadap kode sumber *(Source Code)* sistem dilindungi oleh kontrol akses?	✓	
		2	Apakah perlindungan terhadap source code disetujui oleh manajemen?	✓	
		3	Apakah perlindungan terhadap source code di komunikasikan terhadap seluruh karyawan terkait?		✓
		4	Apakah perlindungan terhadap source code sudah sesuai dengan tujuan dan arahan organisasi?		✓
		5	Apakah dilakukan review terkait perlindungan source code apabila ditemukan perubahan suatu kondisi?	✓	
A.11	Keamanan fisik dan lingkungan		Pertanyaan	Ya	Tidak

Tabel lampiran D. 35 Responden 2 (Lanjutan)

A.11.1	Area aman				
A.11.1.1	Perimeter (pembatas) keamanan fisik	1	Apakah terdapat perimeter (pembatas) keamanan khusus?	✓	
		2	Apakah area informasi sensitif atau kritis dipisahkan dan dikontrol dengan baik?	✓	

		3	Apakah pembatas keamanan fisik sudah sesuai berdasarkan standar keamanan?		✓
		4	Apakah pembatas keamanan fisik dirancang untuk perlindungan terhadap ancaman kejahatan?	✓	
		5	Apakah pembatas fisik dievaluasti apabila ditemukan perubahan kondisi?	✓	
A.11.1.2	Kontrol entri fisik	1	Apakah area aman *(secure area)* memiliki sistem kontrol masuk yang sesuai untuk memastikan hanya personel yang berwenang yang memiliki akses?	✓	
		2	Apakah secure area telah mengikuti standar keamanan?		✓
		3	Apakah kontrol entri sudah sesuai dengan kebijakan organisaisi?	✓	
		4	Apakahpersonel yang dapat masuk ke secure area sudah sesuai dengan kebijakan organisasi?		✓
		5	Apakah kontrol entri terhadap secure area direview apabila ditemukan perubahan terhadap suatu kondisi?	✓	
A.11.1.3	Mengamankan kantor, kamar, dan fasilitas	1	Apakah ruangan kantor dan fasilitas lain telah dirancang dan dikonfigurasi dengan mempertimbangkan keamanan?		✓
		2	Apakah terdapat proses untuk menjaga keamanan (misalnya mengunci, membersihkan meja, dll.)?	✓	
		3	Apak terkait keamanan ruangan sudah dikomunikasikan dengan baik kepada karayawan?		✓
		4	apakah ruangan kantor sudah sesuai dengan suatu standar?		✓
		5	Apakah dilakuna review terhadap keamanan kantor atau ruangan apabila ditemukan perubahan suatu kondisi?	✓	

Tabel lampiran D. 36 Responden 2 (Lanjutan)

A.11.1.4	Melindungi dari ancaman eksternal dan lingkungan	1	Apakah perlindungan fisik untuk mencegah bencana alam, serangan jahat atau kecelakaan telah dirancang?	✓	
		2	Apakah perlindungan fisik terkait ancaman bencana alam atau serangan jahat sudah disetujui oleh manajemen?	✓	

		3	Apakah perlindungan fisik sudah terdukomentasi?		✓
		4	Apakah perlindungan fisik terkait ancaman bencana alam dan pihak jahat sudah sesuai standar keamanan?	✓	
		5	Apakah dilakukan review terkait rancanagan perlindungan fisik apabila ditemukan perubahan suatu kondisi?		✓
A.11.1.5	Bekerja di tempat yang aman	1	Apakah terdapat area aman *(Secure Area)?*	✓	
		2	Apakah s*ecure area* memiliki kebijakan dan proses yang sesuai?	✓	
		3	Apakah kebijakan dan proses dilakukan dan dipantau?		✓
		4	Apakah secure area sudah distujui organisasi?	✓	
		5	Apakah dilakukan review terkait secure area apabila ditemukan perubahan pada suatu kondisi?	✓	
A.11.1.6	Area pengiriman dan pemuatan	1	Apakah terdapat area pengiriman / pemuatan yang terpisah?	✓	
		2	Apakah akses ke area pengiriman/pemuatan dikendalikan?	✓	
		3	Apakah akses area pemuatan diisolasi dari fasilitas pemrosesan informasi?	✓	
		4	Apakah lokasi pemuatan sudah sesuai dengan standar kemanan?	✓	
		5	Apakah area pengiriman dan pemuatan direview apabila ditemukan perubahan suatu kondisi?		✓
A.11.2	Peralatan		Pertanyaan	Ya	Tidak
A.11.2.1	Penempatan dan perlindungan peralatan	1	Apakah bahaya lingkungan diidentifikasi dan dipertimbangkan ketika lokasi peralatan dipilih?		✓
		2	Apakah risiko akses yang tidak sah telah dipertimbangkan saat menentukan lokasi peralatan?	✓	
		3	Apakah penempatan peralatan sudah terdokumentasi?	✓	

Tabel lampiran D. 37 Responden 2 (Lanjutan)

		4	Apakah penempatan peralatan sudah seuasuai dengan kebutuhan organisasi?	✓	
		5	Apaha dilakukan review terkait penempatan dan perlindungan peralatan apabila ditemukan perubahan suatu kondisi?		✓
A.11.2.2	Utilitas pendukung	1	Apakah terdapat UPS atau generator cadangan?	✓	

		2	Apakah sistem UPS sudah diuji dalam skala waktu yang sesuai?	✓	
		3	Apakah UPS yangdigunakan sudah berdasarkan suatu standar?	✓	
		4	Apakah penggunaan UPS sudah berdasarkan kebutuhan organisasi?		✓
		5	Apakah terdapat mekanisme review terkait penggunaan UPS apabila ditemukan perubahan suatu kondisi?	✓	
A.11.2.3	Keamanan kabel	1	Apakah penilaian risiko telah dilakukan atas lokasi kabel listrik dan kabel telekomunikasi atau jaringan?		✓
		2	Apakah kabel listrik dan jaringan ditempatkan supaya terlindung dari gangguan, intersepsi, atau kerusakan?	✓	
		3	Apakah penempatan kabel Istrik dan jaringan sudah terdokumentasi?		✓
		4	Apakah penentuan tempat kabel listrik dan jaringan sudah berdasarkan penilaian ancaman bencana alam dan ancaman pihak jahat?	✓	
		5	Apakah dilakukan review terkait penempatan posisi kabel dan ajaringan apabila ditemukan perubahan suatu kondisi?	✓	
A.11.2.4	Perawatan peralatan	1	Apakah terdapat jadwal perawatan peralatan yang ketat?		✓
		2	Apaakah perawatan peralatan diketahui oleh manajemen?	✓	
		3	Apakah perawatan peralatan terdokumentasi?	✓	
		4	Apakah perawatan peralatan keamanan sudah sesuai dengan standar kemanan?		✓
		5	Apakah dilakukan review terkait terawatan keamanan apabila ditemukan perubahan suatu kondisi?	✓	
A.11.2.5	Penghapusan perangkat	1	Apakah terdapat proses yang mengontrol bagaimana perangkat dihapus dari daftar perangkat?	✓	

Tabel lampiran D. 38 Responden 2 (Lanjutan)

		2	Apakah proses kontol penghapusan perangkat dilakukan?	✓	
		3	Apakah pemeriksaan langsung terhadap proses penghapusan perangkat dilakukan?		✓
		4	Apakah pengahapusan perangkat sudah disetujui oleh manajemen dan pimpinan?		✓
		5	Apakah dilakukan review terkait penghapusan perangkat dari daftar peranghat apabila ditemukan perubahan suatu kondisi?	✓	

A.11.2.6	Keamanan peralatan dan perangkat di luar lokasi	1	Apakah terdapat kebijakan yang mengatur keamanan perangkat di luar lokasi?	✓	
		2	Apakah kebijakan perlindungan perangkat diluar lokasi (kantor) dikomunikasikan secara luas?		✓
		3	Apakah penempatan perlatan diluar lokasi terdokumentasi?		✓
		4	Apakah penempatan perlatan diluar lokasi sudah memperhitungkan bahaya keamanan bencana alam atau ancaman prilaku jahat?		✓
		5	Apakah dilakukan review terkait perlindungan peralatan diluar lokasi?	✓	
A.11.2.7	Pembuangan yang aman atau penggunaan kembali peralatan	1	Apakah terdapat kebijakan yang mengatur bagaimana perangkat informasi dapat digunakan kembali?	✓	
		2	Apakah mekanisme pengelolaan data, diverifikasi dengan benar sebelum digunakan kembali / dibuang?	✓	
		3	Apakah kebijakan penggunaan atau pembuanagan data sudah dikomunikasikan secara baik kepada karyawan?		✓
		4	Apakah pembuangan atau penggunaan kembali peralatan sudah berdasarkan pertimbangan keamanan?	✓	
		5	Apakah terdapat mekanisme review terkait penggunaan atau pembuangan apabila ditemukan perubahan suatu kondisi?	✓	
A.11.2.8	Peralatan pengguna tanpa pengawasan	1	Apakah organisasi memiliki kebijakan tentang bagaimana peralatan yang tidak dijaga harus dilindungi?		✓
		2	Apakah kontrol teknis diterapkan untuk mengamankan peralatan yang secara tidak sengaja ditinggalkan?		✓

Tabel lampiran D. 39 Responden 2 (Lanjutan)

		3	Apakah terdapat pendokumentasian terhadap barang - barang yang tidak sengaja ditinggalkan?	✓	
		4	Apakah kebijakan terkait perlindungan perlatan yang tidak sengaja ditinggalkan sudah diketahui pimpinan dan manajemen?		✓
		5	Apakah dilakukan review terkait kebijakan perlindungan barang yang tdaik sengaja ditinggalkan?	✓	
A.11.2.9	Kebijakan *Clear desk and clear screen*	1	Apakah terdapat kebijakan *clear desk /clear screen?*	✓	

		2	Apakah kebijakan clear desk dan clear screen diberlakukan dengan baik?	✓	
		3	Apakah kebijakan terkait clear screen dan clear desk sudah dikomunikasikan dengan baik dengan karyawan?		✓
		4	Apakah kebijakan clear screen dan clear desk sudah sesuai dengan kebutuhan organisasi?	✓	
		5	Apakah dilakukan review terhadap kebijakan clear screen dan clear desk apabila ditemukan perubahan suatu kondisi?	✓	

Tabel lampiran D. 40 Responden 4

A.5	Kebijakan Keamanan Informasi		Pertanyaan	Ya	Tidak
A.5.1	Arahan manajemen untuk keamanan informasi				
A.5.1.1	Kebijakan untuk keamanan informasi	1	Apakah terdapat kebijakan keamanan informasi terkait pengelolaan informasi?	✓	
		2	Apakah kebijakan keamanan Informasi tersebut disetujui oleh manajemen dan pimpinan?	✓	
		3	Apakah kebijakan dikomunikasikan secara baik kepada karyawan?	✓	
		4	Apakah kebikakan dibuat sesuai dengan tujuan organisasi?		✓

Tabel lampiran D. 41 Responden 2 (Lanjutan)

		5	Apakah kebijakan dapat disesuaikan apabila ditemukan perubahan suatu kondisi?		✓
A.5.1.2	Review kebijakan untuk keamanan informasi	1	Apakah dilakukan peninjauan terhadap kebijakan keamanan informasi?	✓	
		2	Apakah peninjauan dilakunan secara berkala?		✓
		3	Apakah peninjauan melibatkan manajemen dan pimpinan?		✓
		4	Apakah review dilakukan berdasarkan kebutuhan oraganisasi?		✓

		5	Apakah dilakukan review terhadap kebijakan apabila ditemukan perubahan situasi?	✓	
A.6	Keamanan Informasi Organisasi		Pertanyaan	Ya	Tidak
A.6.1	Internal Organisasi				
A.6.1.1	Peran dan tanggung jawab keamanan informasi	1	Apakah tanggung jawab terkait perlindungan perangkat pribadi, untuk melaksanakan proses keamanan, diidentifikasi, dan dikomunikasikan kepada pihak terkait?		✓
		2	Apakah peran dan tanggungjawab telah sesuai dengan keahlian masing - masing karyawan?	✓	
		3	Apakah terdapat dokumentasi terkait pelaksanaan tugas dan tanggungjawab dalam menjaga informasi organisasi?	✓	
		4	Apakah peran dan tanggungjawab karyawan sudah sesuai dengan tujuan organisasi?		✓
		5	Apakah dilakuakan review terkait peran dan tanggungjawab karayawan dalam menjaga keamanan informasi organisasi?	✓	
A.6.1.2	Pemisahan tugas	1	Apakah tugas dan bidang tanggung jawab dipisahkan, untuk mengurangi peluang modifikasi yang tidak sah atau penyalahgunaan informasi, atau layanan?	✓	
		2	Apakah pemisahan tugas sudah sesuai dengan keahlian masing - masing karyawan?	✓	
		3	Apakah pemisahan tugas sudah sesuai dengan kebijakan organisasi?		✓

Tabel lampiran D. 42 Responden 2 (Lanjutan)

		4	Apakah pemisahan tugas, bidang dan tanggungajawab sudah sesuai dengan tujuan atau visi misi organisasi?	✓	
		5	Apakah pemisahan tugas, bidang dan tanggungjawab direview apabila ditemukan perubahan suatu kondisi?	✓	
A.6.1.3	Kontak dengan pihak berwenang	1	Apakah terdapat prosedur yang mendokumentasikan kapan, dan oleh siapa, kontak dengan otoritas terkait akan dilakukan?		✓
		2	Apakah kontak dengan otoritas terkait disetujui oleh manajemen?		✓

		3	Apakah terdapat proses yang merinci bagaimana dan kapan kontak perlu dilakukan?		✓
		4	Apakah terdapat proses untuk kontak rutin dan berbagi pengetahuan?	✓	
		5	Apakah kontak dengan pihak terkait dilakukan secara rutin?		✓
A.6.1.4	Kontak dengan kelompok minat khusus	1	Apakah terdapat pihak yang berwenang untuk mengaktifkan keanggotaan?		✓
		2	Apakah pengaktifan keanggotaan sudah dilakukan oleh pihak yang sesuai?	✓	
		3	Apakah pengaktifan keanggotaan sudah diketahui oleh manajemen dan pimpinan?	✓	
		4	Apakah pengaktifan keanggotaan sesuai atau sejalan dengan tujuan organiasasi?		✓
		5	Apakah dilakukan review terkait pengaktifan keanggotaan apabila ditemukan perubahan suatu kondisi?	✓	
A.6.1.5	Keamanan informasi dalam manajemen proyek	1	Apakah seluruh proyek sudah melalui beberapa penilaian keamanan informasi?		✓
		2	Apakah penilaian terkait keamanan informasi sudah mengacu pada suatu standar?	✓	
		3	Apakah penilaian keamanan informasi terdokumentasi?	✓	
		4	Apakah penilaian keamanan informasi sesuai dengan tujuan organisasi?		✓
		5	Apakah penilaian keamanan informasi pada suatu proyek dilakukan secara rutin sesuai tahapan proyek?		✓

Tabel lampiran D. 43 Responden 2 (Lanjutan)

A.6.2	Perangkat Seluler dan *Teleworking*		Pertanyaan	Ya	Tidak
A.6.2.1	Kebijakan perangkat seluler	1	Apakah terdapat kebijakan terkait perangkat seluler?		✓
		2	Apakah kebijakan terkait perangkat selular mendapat persetujuan manajemen?		✓
		3	Apakah terdapat kebijakan yang mendokumentasikan dan menangani risiko dari penggunaan perangkat seluler (penggunaan hotspot ilegal)?		✓
		4	Apakah kebijakan terkait perangkat selular sesuai dengan tujuan organisasi?		✓

		5	Apakah kebijakan terkait perangkat seluler direview apabila ditemukan perubahan pada suatu kondisi?	✓	
A.6.2.2	*Teleworking*	1	Apakah terdapat kebijakan untuk *teleworking* (kerja diluar kantor) misalnya kerja dari rumah (WFH)?	✓	
		2	Apakah *teleworking* mendapat persetujuan manajemen?	✓	
		3	Apakah terdapat mekanisme atau proses yang ditetapkan bagi pekerja jarak jauh untuk mendapatkan akses (terhadap layanan/sistem)?		✓
		4	Apakah karyawan yang akan melakukan WFH diberi pengarahan terkait perlindungan perangkat yang mereka gunakan?	✓	
		5	Apakah dilakukan review terkait kebijakan WFH apabila ditemukan perubahan suatu kondisi?	✓	
A.9	Kontrol akses		Pertanyaan	Ya	Tidak
A.9.1	Persyaratan bisnis untuk kontrol akses				
A.9.1.1	Kebijakan kontrol akses	1	Apakah terdapat kebijakan kontrol akses?	✓	
		2	Apakah terdapat kebijakan terkait kontrol akses berdasarkan kebutuhan proses bisnis?	✓	
		3	Apakah kebijakan terkait kontrol akses dikomunikasikan dengan baik dengan manajemen?		✓
		4	Apakah kebijakan terkait kontrol akses sudah sesuai dengan tujuan organisasi?	✓	

Tabel lampiran D. 44 Responden 2 (Lanjutan)

		5	Apakah kebijakan terkait kontrol akses di review apabila ditemukan perubahan pada suatu kondisi?	✓	
A.9.1.2	Akses ke jaringan dan layanan jaringan	1	Apakah terdapat kontrol untuk memastikan pengguna hanya memiliki akses ke jaringan khusus yang diperlukan untuk tugas mereka		✓
		2	Apakah kontrol pengguna pada suatu jaringan sudah disetujui manajemen?	✓	
		3	Apakah layanan jaringan sudah dikomunikasikan secara baik kepada pihak terkait?	✓	

		4	Apakah layanan jaringan yang didapatkan pengguna sudah mengacu pada suatu standar?	✓	
		5	Apakah dilakukan perubahan layanan terkait akses jaringan apabila ditemukan perubahan suatu kondisi?		✓
A.9.2	Manajemen akses pengguna		Pertanyaan	Ya	Tidak
A.9.2.1	Pendaftaran pengguna dan pencabutan pendaftaran	1	Apakah terdapat proses pendaftaran akses untuk pengguna secara formal?	✓	
		2	Apakah proses pendaftaran akses untuk pengguna sudah disetujui oleh manajemen?		✓
		3	Apakah proses pendaftaran akses untuk pengguna sudah terdokumentasi?	✓	
		4	Apakah pemberian akses untuk pengguna sudah sesuai dengan tujuan organisasi?	✓	
		5	Apakah akses unntuk pengguna direview apabila ditemukan perubahan suatu kondisi?	✓	
A.9.2.2	Penyediaan akses pengguna	1	Apakah terdapat proses penyediaan akses bagi pengguna untuk menetapkan hak akses semua jenis dan layanan?	✓	
		2	Apakah proses penyediaan akases bagi pengguna sudah disetujui oleh manajemen?	✓	
		3	Apakah penyediaan akses untuk pengguna sudah terdokumentasi?	✓	

Tabel lampiran D. 45 Responden 2 (Lanjutan)

		4	Apakah penyediaan akses untuk pengguna sudah sesuai dengan tujuan organisasi?		✓
		5	Apakah dilakukan review terkait penyediaan akses untuk pengguna apabila ditemukan perubahan suatu kondisi?		✓
A.9.2.3	Pengelolaan hak akses istimewa	1	Apakah akun dengan akses istimewa (admin dan super admin) dikelola dan dikontrol secara terpisah?	✓	
		2	Apakah pengelolaan akses super admin dan super admin mengacu pada suatu standar keamanan?	✓	

		3	Apakah pengelolaan akun admin dan super admin sudah terdokumentasi?	✓	
		4	Apakah pengelolaan akun admin dan super admin sudah sesuai dengan tujuan organisasi?	✓	
		5	Apakah dilakukan review terkait pengelolaan akun admin dan superadmin apabila ditemukan perubahan suatu kondisi?	✓	
A.9.2.4	Pengelolaan informasi otentikasi rahasia pengguna	1	Apakah terdapat proses manajemen secara formal untuk mengontrol informasi rahasia?		✓
		2	Apakah pengelolaan informasi rahasia pengguna sudah mengacu pada suatu standar keamanan?	✓	
		3	Apakah mekanisme pengelolaan data rahasia pengguna telah dikomunikasikan secara baik kepada seluruh karyawan terkait?	✓	
		4	Apakah proses pengelolaan data rahasia pengguna diketahui oleh manajemen?		✓
		5	Apak dialakukan review terkait pengelolaan data rahasia pengguna apabila ditemukan perubahan kondisi?	✓	
A.9.2.5	Review hak akses pengguna	1	Apakah terdapat proses bagi pemilik perangkat untuk meninjau hak akses ke perangkat mereka secara teratur?	✓	
		2	Apakah proses tinjauan ini diverifikasi?		✓
		3	ApaKah proses review terdokumentasi?	✓	

Tabel lampiran D. 46 Responden 2 (Lanjutan)

		4	Apakah proses review terkait hak akses pengguna mendapat persetujuan manajemen?	✓	
		5	Apakah proses review sudah sesuai dengan tujuan organisasi?	✓	
A.9.2.6	Penghapusan atau penyesuaian hak akses	1	Apakah terdapat mekanisme dan proses untuk memastikan hak akses pengguna dihapus saat pemutusan hubungan kerja, atau saat perubahan peran?	✓	
		2	Apakah proses untuk penghapusan hak akses sudah diketahui oleh manajemen?	✓	

		3	Apakah proses penghapusan kah akses terdokumentasi?		✓
		4	Apakah proses penghapusan dan penyesuaian hak akses sudah sesuai dengan tujuan oraganisasi?	✓	
		5	Apakah dilakukan review terkait proses penghapusan dan penyesuaian hak akses apabila ditemukan perubahan suatu kondisi?	✓	
A.9.3	Tanggung jawab pengguna		Pertanyaan	Ya	Tidak
A.9.3.1	Penggunaan informasi otentikasi rahasia	1	Apakah terdapat dokumen kebijakan yang mencakup praktik organisasi tentang bagaimana informasi otentikasi rahasia harus ditangani?		✓
		2	Dokumen tersebut dikomunikasikan kepada semua pengguna		✓
		3	Apakah dokumen tersebut mengacu pada sebuah standar keamanan?		✓
		4	Apakah penanganan informasi rahasia sudah sesuai denagan tujuan organisasi?	✓	
		5	Apakah dilakukan review terhadap dokumen yang berisi tentang penanganan informasi rahasia pengguna apabila ditemukan perubahan suatu kondisi?	✓	
A.9.4	Kontrol akses sistem dan aplikasi		Pertanyaan	Ya	Tidak
A.9.4.1	Pembatasan akses informasi	1	Apakah akses terhadap informasi dan fungsi sistem aplikasi dibatasi sesuai dengan kebijakan kontrol akses?	✓	
		2	Apakah pembatasan akses terhadap informasi dan fungsi aplikasi disetujui oleh manajemen?	✓	

Tabel lampiran D. 47 Responden 2 (Lanjutan)

		3	Apakah pembatasan akses terhadap inforamasi dan fungsi aplikasi sudah dikomunikasikan kepada seluruh karyawan?		✓
		4	Apakah pembatasan akses terhadap inforamasi dan fungsi aplikasi sesuai dengan tujuan organisasi?	✓	
		5	Apakah dilakuakan review terkait pembatasan informasi dan fungsi apalikasi apabila ditemukan perubahan suatu kondisi?	✓	
A.9.4.2	Amankan prosedur log-on	1	Apakah akses dikontrol oleh prosedur log-on yang aman?		✓

		2	Apakah prosedur log-on sudah mengacu pada suatu standar keamanan?	✓	
		3	Apakah terdapat mekanisme yang mendokumentasikan prosedur log-on?		✓
		4	apakah prosedur log-on dirancang agar terhindar dari gangguan pihak jahat?	✓	
		5	Apakah terdapat mekanisme review terkait keamanan prosedur log-on apabila dietemukan isu atau perubahan suatu kondisi?	✓	
A.9.4.3	Sistem manajemen kata sandi	1	Apakah sistem kata sandi bersifat interaktif?	✓	
		2	Apakah diperlukan kata sandi yang rumit?		✓
		3	Apakah manajemen kata sandi sudah mengacu pada suatu standar keamanan?		✓
		4	Apakah terdapat kewajiban untuk mengganti kata sandi secara rutin?		✓
		5	Apakah manajemen pengelolaan kata sandi direview apabila ditemukan perubahan suatu kondisi?	✓	
A.9.4.4	Penggunaan program utilitas dengan hak istimewa	1	Apakah program utilitas hak istimewa dibatasi dan dipantau?	✓	
		2	Apakah penggunaan program utilitas dengan hak istimewa sudah disetujui oleh manajemen?	✓	
		3	Apakah penggunaan program utilitas dengan hak istimewa sudah terdokumentasi?	✓	

Tabel lampiran D. 48 Responden 2 (Lanjutan)

		4	Apakah penggunaan program utilitas dengan hak istimewa sudah sesuai dengan kebijakan dan tujuan organisasi?	✓	
		5	Apakah dilakuna review terkait penggunaan program utilitas dengan hak akses istimewa apabila ditemukan perubahan suatu kondisi?		✓
A.9.4.5	Kontrol akses ke kode sumber program	1	Apakah akses terhadap kode sumber *(Source Code)* sistem dilindungi oleh kontrol akses?	✓	
		2	Apakah perlindungan terhadap source code disetujui oleh manajemen?	✓	

		3	Apakah perlindungan terhadap source code di komunikasikan terhadap seluruh karyawan terkait?		✓
		4	Apakah perlindungan terhadap source code sudah sesuai dengan tujuan dan arahan organisasi?	✓	
		5	Apakah dilakukan review terkait perlindungan source code apabila ditemukan perubahan suatu kondisi?	✓	
A.11	Keamanan fisik dan lingkungan		Pertanyaan	Ya	Tidak
A.11.1	Area aman				
A.11.1.1	Perimeter (pembatas) keamanan fisik	1	Apakah terdapat perimeter (pembatas) keamanan khusus?	✓	
		2	Apakah area informasi sensitif atau kritis dipisahkan dan dikontrol dengan baik?	✓	
		3	Apakah pembatas keamanan fisik sudah sesuai berdasarkan standar keamanan?	✓	
		4	Apakah pembatas keamanan fisik dirancang untuk perlindungan terhadap ancaman kejahatan?	✓	
		5	Apakah pembatas fisik dievaluasti apabila ditemukan perubahan kondisi?	✓	
A.11.1.2	Kontrol entri fisik	1	Apakah area aman *(secure area)* memiliki sistem kontrol masuk yang sesuai untuk memastikan hanya personel yang berwenang yang memiliki akses?	✓	
		2	Apakah secure area telah mengikuti standar keamanan?	✓	
		3	Apakah kontrol entri sudah sesuai dengan kebijakan organisaisi?		✓

Tabel lampiran D. 49 Responden 2 (Lanjutan)

		4	Apakah personel yang dapat masuk ke secure area sudah sesuai dengan kebijakan organisasi?	✓	
		5	Apakah kontrol entri terhadap secure area direview apabila ditemukan perubahan terhadap suatu kondisi?	✓	
A.11.1.3	Mengamankan kantor, kamar, dan fasilitas	1	Apakah ruangan kantor dan fasilitas lain telah dirancang dan dikonfigurasi dengan mempertimbangkan keamanan?		✓
		2	Apakah terdapat proses untuk menjaga keamanan (misalnya mengunci, membersihkan meja, dll.)?	✓	

		3	Apakah terkait keamanan ruangan sudah dikomunikasikan dengan baik kepada karayawan?	✓	
		4	Apakah ruangan kantor sudah sesuai dengan suatu standar?		✓
		5	Apakah dilakuna review terhadap keamanan kantor atau ruangan apabila ditemukan perubahan suatu kondisi?	✓	
A.11.1.4	Melindungi dari ancaman eksternal dan lingkungan	1	Apakah perlindungan fisik untuk mencegah bencana alam, serangan jahat atau kecelakaan telah dirancang?		✓
		2	Apakah perlindungan fisik terkait ancaman bencana alam atau serangan jahat sudah disetujui oleh manajemen?	✓	
		3	Apakah perlindungan fisik sudah terdukomentasi?		✓
		4	Apakah perlindungan fisik terkait ancaman bencana alam dan pihak jahat sudah sesuai standar keamanan?	✓	
		5	Apakah dilakukan review terkait rancanagan perlindungan fisik apabila ditemukan perubahan suatu kondisi?	✓	
A.11.1.5	Bekerja di tempat yang aman	1	Apakah terdapat area aman *(Secure Area)?*	✓	
		2	Apakah s*ecure area* memiliki kebijakan dan proses yang sesuai?	✓	
		3	Apakah kebijakan dan proses dilakukan dan dipantau?		✓
		4	Apakah secure area sudah distujui organisasi?	✓	
		5	Apakah dilakukan review terkait secure area apabila ditemukan perubahan pada suatu kondisi?	✓	
A.11.1.6	Area pengiriman dan pemuatan	1	Apakah terdapat area pengiriman / pemuatan yang terpisah?	✓	

Tabel lampiran D. 50 Responden 2 (Lanjutan)

		2	Apakah akses ke area pengiriman/pemuatan dikendalikan?	✓	
		3	Apakah akses area pemuatan diisolasi dari fasilitas pemrosesan informasi?	✓	
		4	Apakah secure area sudah distujui organisasi?	✓	
		5	Apakah dilakukan review terkait secure area apabila ditemukan perubahan pada suatu kondisi?	✓	
A.11.2	Peralatan		Pertanyaan	Ya	Tidak

A.11.2.1	Penempatan dan perlindungan peralatan	1	Apakah bahaya lingkungan diidentifikasi dan dipertimbangkan ketika lokasi peralatan dipilih?		✓
		2	Apakah risiko akses yang tidak sah telah dipertimbangkan saat menentukan lokasi peralatan?	✓	
		3	Apakah penempatan peralatan sudah terdokumentasi?		✓
		4	Apakah penempatan peralatan sudah seuasuai dengan kebutuhan organisasi?	✓	
		5	Apaha dilakukan review terkait penempatan dan perlindungan peralatan apabila ditemukan perubahan suatu kondisi?	✓	
A.11.2.2	Utilitas pendukung	1	Apakah terdapat UPS atau generator cadangan?	✓	
		2	Apakah sistem UPS sudah diuji dalam skala waktu yang sesuai?		✓
		3	Apakah UPS yangdigunakan sudah berdasarkan suatu standar?	✓	
		4	Apakah penggunaan UPS sudah berdasarkan kebutuhan organisasi?		✓
		5	Apakah terdapat mekanisme review terkait penggunaan UPS apabila ditemukan perubahan suatu kondisi?	✓	
A.11.2.3	Keamanan kabel	1	Apakah penilaian risiko telah dilakukan atas lokasi kabel listrik dan kabel telekomunikasi atau jaringan?		✓
		2	Apakah kabel listrik dan jaringan ditempatkan supaya terlindung dari gangguan, intersepsi, atau kerusakan?	✓	
		3	Apakah penempatan kabel lstrik dan jaringan sudah terdokumentasi?		✓

Tabel lampiran D. 51 Responden 2 (Lanjutan)

		4	Apakah penentuan tempat kabel listrik dan jaringan sudah berdasarkan penilaian ancaman bencana alam dan ancaman pihak jahat?	✓	
		5	Apakah dilakukan review terkait penempatan posisi kabel dan ajaringan apabila ditemukan perubahan suatu kondisi?		✓
A.11.2.4	Perawatan peralatan	1	Apakah terdapat jadwal perawatan peralatan yang ketat?		✓
		2	Apakah perawatan peralatan diketahui oleh manajemen?	✓	
		3	Apakah perawatan peralatan terdokumentasi?	✓	

		4	Apakah perawatan peralatan keamanan sudah sesuai dengan standar kemanan?		✓□
		5	Apakah dilakukan review terkait terawatan keamanan apabila ditemukan perubahan suatu kondisi?	✓□	
A.11.2.5	Penghapusan perangkat	1	Apakah terdapat proses yang mengontrol bagaimana perangkat dihapus dari daftar perangkat?	✓□	
		2	Apakah proses kontol penghapusan perangkat dilakukan?	✓□	
		3	Apakah pemeriksaan langsung terhadap proses penghapusan perangkat dilakukan?		✓□
		4	Apakah pengahapusan perangkat sudah disetujui oleh manajemen dan pimpinan?	✓□	
		5	Apakah dilakukan review terkait penghapusan perangkat dari daftar peranghat apabila ditemukan perubahan suatu kondisi?	✓□	
A.11.2.6	Keamanan peralatan dan perangkat di luar lokasi	1	Apakah terdapat kebijakan yang mengatur keamanan perangkat di luar lokasi?	✓□	
		2	Apakah kebijakan perlindungan perangkat diluar lokasi (kantor) dikomunikasikan secara luas?		✓□
		3	Apakah penempatan perlatan diluar lokasi terdokumentasi?		✓□
		4	Apakah penempatan perlatan diluar lokasi sudah memperhitungkan bahaya keamanan bencana alam atau ancaman prilaku jahat?	✓□	
		5	Apakah dilakukan review terkait perlindungan peralatan diluar lokasi?	✓□	

Tabel lampiran D. 52 Responden 2 (Lanjutan)

A.11.2.7	Pembuangan yang aman atau penggunaan kembali peralatan	1	Apakah terdapat kebijakan yang mengatur bagaimana perangkat informasi dapat digunakan kembali?	✓□	
		2	Apakah mekanisme pengelolaan data, diverifikasi dengan benar sebelum digunakan kembali / dibuang?		✓□
		3	Apakah kebijakan penggunaan atau pembuanagan data sudah dikomunikasikan secara baik kepada karyawan?	✓□	

		4	Apakah pembuangan atau penggunaan kembali peralatan sudah berdasarkan pertimbangan keamanan?	✓	
		5	Apakah terdapat mekanisme review terkait penggunaan atau pembuangan apabila ditemukan perubahan suatu kondisi?	✓	
A.11.2.8	Peralatan pengguna tanpa pengawasan	1	Apakah organisasi memiliki kebijakan tentang bagaimana peralatan yang tidak dijaga harus dilindungi?	✓	
		2	Apakah kontrol teknis diterapkan untuk mengamankan peralatan yang secara tidak sengaja ditinggalkan?		✓
		3	Apakah terdapat pendokumentasian terhadap barang - barang yang tidak sengaja ditinggalkan?		✓
		4	Apakah kebijakan terkait perlindungan perlatan yang tidak sengaja ditinggalkan sudah diketahui pimpinan dan manajemen?	✓	
		5	Apakah dilakukan review terkait kebijakan perlindungan barang yang tdaik sengaja ditinggalkan?	✓	
A.11.2.9	Kebijakan *Clear desk and clear screen*	1	Apakah terdapat kebijakan *clear desk /clear screen?*	✓	
		2	Apakah kebijakan clear desk dan clear screen diberlakukan dengan baik?		✓
		3	Apakah kebijakan terkait clear screen dan clear desk sudah dikomunikasikan dengan baik dengan karyawan?	✓	
		4	Apakah kebijakan clear screen dan clear desk sudah sesuai dengan kebutuhan organisasi?	✓	
		5	Apakah dilakukan review terhadap kebijakan clear screen dan clear desk apabila ditemukan perubahan suatu kondisi?	✓	

Tabel lampiran D. 53 Responden 5

A.5	Kebijakan Keamanan Informasi		Pertanyaan	Ya	Tidak
A.5.1	Arahan manajemen untuk keamanan informasi				
A.5.1.1	Kebijakan untuk keamanan informasi	1	Apakah terdapat kebijakan keamanan informasi terkait pengelolaan informasi?	✓	

		2	Apakah kebijakan keamanan Informasi tersebut disetujui oleh manajemen dan pimpinan?	✓	
		3	Apakah kebijakan dikomunikasikan secara baik kepada karyawan?		✓
		4	Apakah kebijakan dibuat sesuai dengan tujuan organisasi?	✓	
		5	Apakah kebijakan dapat disesuaikan apabila ditemukan perubahan suatu kondisi?		✓
A.5.1.2	Review kebijakan untuk keamanan informasi	1	Apakah dilakukan peninjauan terhadap kebijakan keamanan informasi?		✓
		2	Apakah peninjauan dilakunan secara berkala?		✓
		3	Apakah peninjauan melibatkan manajemen dan pimpinan?		✓
		4	Apakah review dilakukan berdasarkan kebutuhan oraganisasi?		✓
		5	Apakah dilakukan review terhadap kebijakan apabila ditemukan perubahan situasi?	✓	
A.6	Keamanan Informasi Organisasi		Pertanyaan	Ya	Tidak
A.6.1	Internal Organisasi				
A.6.1.1	Peran dan tanggung jawab keamanan informasi	1	Apakah tanggung jawab terkait perlindungan perangkat pribadi, untuk melaksanakan proses keamanan, diidentifikasi, dan dikomunikasikan kepada pihak terkait?	✓	
		2	Apakah peran dan tanggungjawab telah sesuai dengan keahlian masing - masing karyawan?		✓
		3	Apakah terdapat dokumentasi terkait pelaksanaan tugas dan tanggungjawab dalam menjaga informasi organisasi?		✓
		4	Apakah peran dan tanggungjawab karyawan sudah sesuai dengan tujuan organisasi?	✓	

Tabel lampiran D. 54 Responden 5 (Lanjutan)

		5	Apakah dilakuakan review terkait peran dan tanggungjawab karayawan dalam menjaga keamanan informasi organisasi?	✓	
A.6.1.2	Pemisahan tugas	1	Apakah tugas dan bidang tanggung jawab dipisahkan, untuk mengurangi peluang modifikasi yang tidak sah atau penyalahgunaan informasi, atau layanan?	✓	

		2	Apakah pemisahan tugas sudah sesuai dengan keahlian masing - masing karyawan?		✓
		3	Apakah pemisahan tugas sudah sesuai dengan kebijakan organisasi?	✓	
		4	Apakah pemisahan tugas, bidang dan tanggungajawab sudah sesuai dengan tujuan atau visi misi organisasi?		✓
		5	Apakah pemisahan tugas, bidang dan tanggungjawab direview apabila ditemukan perubahan suatu kondisi?	✓	
A.6.1.3	Kontak dengan pihak berwenang	1	Apakah terdapat prosedur yang mendokumentasikan kapan, dan oleh siapa, kontak dengan otoritas terkait akan dilakukan?	✓	
		2	Apakah kontak dengan otoritas terkait disetujui olem manajemen?		✓
		3	Apakah terdapat proses yang merinci bagaimana dan kapan kontak perlu dilakukan?		✓
		4	Apakah terdapat proses untuk kontak rutin dan berbagi pengetahuan?	✓	
		5	Apakah kontak dengan pihak terkait dilakukan secara rutin?	✓	
A.6.1.4	Kontak dengan kelompok minat khusus	1	Apakah terdapat pihak yang berwenang untuk mengaktifkan keanggotaan?	✓	
		2	Apakah pengaktifan keanggotaan sudah dilakukan oleh pihak yang sesuai?	✓	
		3	Apakah pengaktifan keanggotaan sudah diketahui oleh manajemen dan pimpinan?		✓
		4	Apakah pengaktifan keanggotaan sesuai atau sejalan dengan tujuan organiasasi?		✓
		5	Apakah dilakukan review terkait pengaktifan keanggotaan apabila ditemukan perubahan suatu kondisi?	✓	

Tabel lampiran D. 55 Responden 5 (Lanjutan)

A.6.1.5	Keamanan informasi dalam manajemen proyek	1	Apakah seluruh proyek sudah melalui beberapa penilaian keamanan informasi?	✓	
		2	Apakah penilaian terkait keamanan informasi sudah mengacu pada suatu standar?	✓	
		3	Apakah penilaian keamanan informasi terdokumentasi?		✓
		4	Apakah penilaian keamanan informasi sesuai dengan tujuan organisasi?		✓

		5	Apakah penilaian keamanan informasi pada suatu proyek dilakukan secara rutin sesuai tahapan proyek?	✓□	
A.6.2	Perangkat Seluler dan *Teleworking*		Pertanyaan	Ya	Tidak
A.6.2.1	Kebijakan perangkat seluler	1	Apakah terdapat kebijakan terkait perangkat seluler?	✓□	
		2	Apakah kebijakan terkait perangkat selular mendapat persetujuan manajemen?	✓□	
		3	Apakah terdapat kebijakan yang mendokumentasikan dan menangani risiko dari penggunaan perangkat seluler (penggunaan hotspot ilegal)?		✓□
		4	Apakah kebijakan terkait perangkat selular sesuai dengan tujuan organisasi?		✓□
		5	Apakah kebijakan terkait perangkat seluler direview apabila ditemukan perubahan pada suatu kondisi?		✓□
A.6.2.2	*Teleworking*	1	Apakah terdapat kebijakan untuk *teleworking* (kerja diluar kantor) misalnya kerja dari rumah (WFH)?	✓□	
		2	Apakah *teleworking* mendapat persetujuan manajemen?	✓□	
		3	Apakah terdapat mekanisme atau proses yang ditetapkan bagi pekerja jarak jauh untuk mendapatkan akses (terhadap layanan/sistem)?	✓□	
		4	Apakah karyawan yang akan melakukan WFH diberi pengarahan terkait perlindungan perangkat yang mereka gunakan?		✓□
		5	Apakah dilakukan review terkait kebijakan WFH apabila ditemukan perubahan suatu kondisi?	✓□	
A.9	Kontrol akses		Pertanyaan	Ya	Tidak
A.9.1	Persyaratan bisnis untuk kontrol akses				

Tabel lampiran D. 56 Responden 5 (Lanjutan)

A.9.1.1	Kebijakan kontrol akses	1	Apakah terdapat kebijakan kontrol akses?	✓□	
		2	Apakah terdapat kebijakan terkait kontrol akses berdasarkan kebutuhan proses bisnis?	✓□	
		3	Apakah kebijakan terkait kontrol akses dikomunikasikan dengan baik dengan manajemen?		✓□
		4	Apakah kebijakan terkait kontrol akses sudah sesuai dengan tujuan organisasi?	✓□	

		5	Apakah kebijakan terkait kontrol akses di review apabila ditemukan perubahan pada suatu kondisi?	✓	
A.9.1.2	Akses ke jaringan dan layanan jaringan	1	Apakah terdapat kontrol untuk memastikan pengguna hanya memiliki akses ke jaringan khusus yang diperlukan untuk tugas mereka	✓	
		2	Apakah kontrol pengguna pada suatu jaringan sudah disetujui manajemen?		✓
		3	Apakah layanan jaringan sudah dikomunikasikan secara baik kepada pihak terkait?		✓
		4	Apakah layanan jaringan yang didapatkan pengguna sudah mengacu pada suatu standar?		✓
		5	Apakah dilakukan perubahan layanan terkait akses jaringan apabila ditemukan perubahan suatu kondisi?	✓	
A.9.2	Manajemen akses pengguna		Pertanyaan	Ya	Tidak
A.9.2.1	Pendaftaran pengguna dan pencabutan pendaftaran	1	Apakah terdapat proses pendaftaran akses untuk pengguna secara formal?	✓	
		2	Apakah proses pendaftaran akses untuk pengguna sudah disetujui oleh manajemen?	✓	
		3	Apakah proses pendaftaran akses untuk pengguna sudah terdokumentasi?		✓
		4	Apakah pemberian akses untuk pengguna sudah sesuai dengan tujuan organisasi?	✓	

Tabel lampiran D. 57 Responden 5 (Lanjutan)

		5	Apakah akses unntuk pengguna direview apabila ditemukan perubahan suatu kondisi?	✓	
A.9.2.2	Penyediaan akses pengguna	1	Apakah terdapat proses penyediaan akses bagi pengguna untuk menetapkan hak akses semua jenis dan layanan?	✓	
		2	Apakah proses penyediaan akases bagi pengguna sudah disetujui oleh manajemen?	✓	
		3	Apakah penyediaan akses untuk pengguna sudah terdokumentasi?		✓

		4	Apakah penyediaan akses untuk pengguna sudah sesuai dengan tujuan organisasi?	✓	
		5	Apakah dilakukan review terkait penyediaan akses untuk pengguna apabila ditemukan perubahan suatu kondisi?	✓	
A.9.2.3	Pengelolaan hak akses istimewa	1	Apakah akun dengan akses istimewa (admin dan super admin) dikelola dan dikontrol secara terpisah?	✓	
		2	Apakah pengelolaan akses super admin dan super admin mengacu pada suatu standar keamanan?		✓
		3	Apakah pengelolaan akun admin dan super admin sudah terdokumentasi?		✓
		4	Apakah pengelolaan akun admin dan super admin sudah sesuai dengan tujuan organisasi?		✓
		5	Apakah dilakukan review terkait pengelolaan akun admin dan superadmin apabila ditemukan perubahan suatu kondisi?	✓	
A.9.2.4	Pengelolaan informasi otentikasi rahasia pengguna	1	Apakah terdapat proses manajemen secara formal untuk mengontrol informasi rahasia?		✓
		2	Apakah pengelolaan informasi rahasia pengguna sudah mengacu pada suatu standar keamanan?		✓
		3	Apakah mekanisme pengelolaan data rahasia pengguna telah dikomunikasikan secara baik kepada seluruh karyawan terkait?		✓
		4	Apakah proses pengelolaan data rahasia pengguna diketahui oleh manajemen?		✓

Tabel lampiran D. 58 Responden 5 (Lanjutan)

		5	Apak dialakukan review terkait pengelolaan data rahasia pengguna apabila ditemukan perubahan kondisi?	✓	
A.9.2.5	Review hak akses pengguna	1	Apakah terdapat proses bagi pemilik perangkat untuk meninjau hak akses ke perangkat mereka secara teratur?		✓
		2	Apakah proses tinjauan ini diverifikasi?		✓
		3	Apakah proses review terdokumentasi?		✓

		4	Apakah proses review terkait hak akses pengguna mendapat persetujuan manajemen?		✓□
		5	Apakah proses review sudah sesuai dengan tujuan organisasi?		✓□
A.9.2.6	Penghapusan atau penyesuaian hak akses	1	Apakah terdapat mekanisme dan proses untuk memastikan hak akses pengguna dihapus saat pemutusan hubungan kerja, atau saat perubahan peran?		✓□
		2	Apakah proses untuk penghapusan hak akses sudah diketahui oleh manajemen?		✓□
		3	Apakah proses penghapusan kah akses terdokumentasi?		✓□
		4	Apakah proses penghapusan dan penyesuaian hak akses sudah sesuai dengan tujuan oraganisasi?		✓□
		5	Apakah dilakukan review terkait proses penghapusan dan penyesuaian hak akses apabila ditemukan perubahan suatu kondisi?	✓□	
A.9.3	Tanggung jawab pengguna		Pertanyaan	Ya	Tidak
A.9.3.1	Penggunaan informasi otentikasi rahasia	1	Apakah terdapat dokumen kebijakan yang mencakup praktik organisasi tentang bagaimana informasi otentikasi rahasia harus ditangani?		✓□
		2	Dokumen tersebut dikomunikasikan kepada semua pengguna		✓□
		3	Apakah dokumen tersebut mengacu pada sebuah standar keamanan?		✓□
		4	Apakah penanganan informasi rahasia sudah sesuai denagan tujuan organisasi?		✓□
		5	Apakah dilakukan review terhadap dokumen yang berisi tentang penanganan informasi rahasia pengguna apabila ditemukan perubahan suatu kondisi?	✓□	

Tabel lampiran D. 59 Responden 5 (Lanjutan)

A.9.4	Kontrol akses sistem dan aplikasi		Pertanyaan	Ya	Tidak
A.9.4.1	Pembatasan akses informasi	1	Apakah akses terhadap informasi dan fungsi sistem aplikasi dibatasi sesuai dengan kebijakan kontrol akses?	✓□	
		2	Apakah pembatasan akses terhadap informasi dan fungsi aplikasi disetujui oleh manajemen?		✓□
		3	Apakah pembatasan akses terhadap inforamasi dan fungsi aplikasi sudah dikomunikasikan kepada seluruh karyawan?		✓□

		4	Apakah pembatasan akses terhadap inforamasi dan fungsi aplikasi sesuai dengan tujuan organisasi?	✓	
		5	Apakah dilakuakan review terkait pembatasan informasi dan fungsi apalikasi apabila ditemukan perubahan suatu kondisi?	✓	
A.9.4.2	Amankan prosedur log-on	1	Apakah akses dikontrol oleh prosedur log-on yang aman?	✓	
		2	Apaakah prosedur log-on sudah mengacu pada suatu standar keamanan?		✓
		3	Apakah terdapat mekanisme yang mendokumentasikan prosedur log-on?		✓
		4	apakah prosedur log-on dirancang agar terhindar dari gangguan pihak jahat?	✓	
		5	Apakah terdapat mekanisme review terkait keamanan prosedur log-on apabila dietemukan isu atau perubahan suatu kondisi?	✓	
A.9.4.3	Sistem manajemen kata sandi	1	Apakah sistem kata sandi bersifat interaktif?	✓	
		2	Apakah diperlukan kata sandi yang rumit?		✓
		3	Apakah manajemen kata sandi sudah mengacu pada suatu standar keamanan?		✓
		4	Apakah terdapat kewajiban untuk mengganti kata sandi secara rutin?		✓
		5	Apakah manajemen pengelolaan kata sandi direview apabila ditemukan perubahan suatu kondisi?	✓	
A.9.4.4	Penggunaan program utilitas dengan hak istimewa	1	Apakah program utilitas hak istimewa dibatasi dan dipantau?	✓	

Tabel lampiran D. 60 Responden 5 (Lanjutan)

		2	Apakah penggunaan program utilitas dengan hak istimewa sudah disetujui oleh manajemen?	✓	
		3	Apakah penggunaan program utilitas dengan hak istimewa sudah terdokumentasi?		✓
		4	Apakah penggunaan program utilitas dengan hak istimewa sudah sesuai dengan kebijakan dan tujuan organisasi?	✓	
		5	Apakah dilakuna review terkait penggunaan program utilitas dengan hak akses istimewa apabila ditemukan perubahan suatu kondisi?	✓	

A.9.4.5	Kontrol akses ke kode sumber program	1	Apakah akses terhadap kode sumber *(Source Code)* sistem dilindungi oleh kontrol akses?	✓	
		2	Apakah perlindungan terhadap source code disetujui oleh manajemen?	✓	
		3	Apakah perlindungan terhadap source code di komunikasikan terhadap seluruh karyawan terkait?		✓
		4	Apakah perlindungan terhadap source code sudah sesuai dengan tujuan dan arahan organisasi?	✓	
		5	Apakah dilakukan review terkait perlindungan source code apabila ditemukan perubahan suatu kondisi?	✓	
A.11	Keamanan fisik dan lingkungan		Pertanyaan	Ya	Tidak
A.11.1	Area aman				
A.11.1.1	Perimeter (pembatas) keamanan fisik	1	Apakah terdapat perimeter (pembatas) keamanan khusus?	✓	
		2	Apakah area informasi sensitif atau kritis dipisahkan dan dikontrol dengan baik?		✓
		3	Apakah pembatas keamanan fisik sudah sesuai berdasarkan standar keamanan?		✓
		4	Apakah pembatas keamanan fisik dirancang untuk perlindungan terhadap ancaman kejahatan?	✓	
		5	Apakah pembatas fisik dievaluasti apabila ditemukan perubahan kondisi?	✓	

Tabel lampiran D. 61 Responden 5 (Lanjutan)

A.11.1.2	Kontrol entri fisik	1	Apakah area aman *(secure area)* memiliki sistem kontrol masuk yang sesuai untuk memastikan hanya personel yang berwenang yang memiliki akses?	✓	
		2	Apakah secure area telah mengikuti standar keamanan?		✓
		3	Apakah kontrol entri sudah sesuai dengan kebijakan organisaisi?	✓	
		4	Apakahpersonel yang dapat masuk ke secure area sudah sesuai dengan kebijakan organisasi?		✓

		5	Apakah kontrol entri terhadap secure area direview apabila ditemukan perubahan terhadap suatu kondisi?	✓	
A.11.1.3	Mengamankan kantor, kamar, dan fasilitas	1	Apakah ruangan kantor dan fasilitas lain telah dirancang dan dikonfigurasi dengan mempertimbangkan keamanan?	✓	
		2	Apakah terdapat proses untuk menjaga keamanan (misalnya mengunci, membersihkan meja, dll.)?	✓	
		3	Apak terkait keamanan ruangan sudah dikomunikasikan dengan baik kepada karayawan?		✓
		4	apakah ruangan kantor sudah sesuai dengan suatu standar?	✓	
		5	Apakah dilakuna review terhadap keamanan kantor atau ruangan apabila ditemukan perubahan suatu kondisi?	✓	
A.11.1.4	Melindungi dari ancaman eksternal dan lingkungan	1	Apakah perlindungan fisik untuk mencegah bencana alam, serangan jahat atau kecelakaan telah dirancang?	✓	
		2	Apakah perlindungan fisik terkait ancaman bencana alam atau serangan jahat sudah disetujui oleh manajemen?		✓
		3	Apakah perlindungan fisik sudah terdukomentasi?		✓
		4	Apakah perlindungan fisik terkait ancaman bencana alam dan pihak jahat sudah sesuai standar keamanan?	✓	
		5	Apakah dilakukan review terkait rancanagan perlindungan fisik apabila ditemukan perubahan suatu kondisi?	✓	
A.11.1.5	Bekerja di tempat yang aman	1	Apakah terdapat area aman *(Secure Area)?*	✓	
		2	Apakah s*ecure area* memiliki kebijakan dan proses yang sesuai?	✓	

Tabel lampiran D. 62 Responden 5 (Lanjutan)

		3	Apakah kebijakan dan proses dilakukan dan dipantau?		✓
		4	Apakah secure area sudah distujui organisasi?		✓
		5	Apakah dilakukan review terkait secure area apabila ditemukan perubahan pada suatu kondisi?	✓	
A.11.1.6	Area pengiriman dan pemuatan	1	Apakah terdapat area pengiriman / pemuatan yang terpisah?	✓	
		2	Apakah akses ke area pengiriman/pemuatan dikendalikan?	✓	
		3	Apakah akses area pemuatan diisolasi dari fasilitas pemrosesan informasi?	✓	

		4	Apakah secure area sudah distujui organisasi?	✓	
		5	Apakah dilakukan review terkait secure area apabila ditemukan perubahan pada suatu kondisi?	✓	
A.11.2	Peralatan		Pertanyaan	Ya	Tidak
A.11.2.1	Penempatan dan perlindungan peralatan	1	Apakah bahaya lingkungan diidentifikasi dan dipertimbangkan ketika lokasi peralatan dipilih?	✓	
		2	Apakah risiko akses yang tidak sah telah dipertimbangkan saat menentukan lokasi peralatan?		✓
		3	Apakah penempatan peralatan sudah terdokumentasi?		✓
		4	Apakah penempatan peralatan sudah seuasuai dengan kebutuhan organisasi?	✓	
		5	Apaha dilakukan review terkait penempatan dan perlindungan peralatan apabila ditemukan perubahan suatu kondisi?	✓	
A.11.2.2	Utilitas pendukung	1	Apakah terdapat UPS atau generator cadangan?	✓	
		2	Apakah sistem UPS sudah diuji dalam skala waktu yang sesuai?	✓	
		3	Apakah UPS yangdigunakan sudah berdasarkan suatu standar?		✓
		4	Apakah penggunaan UPS sudah berdasarkan kebutuhan organisasi?	✓	
		5	Apakah terdapat mekanisme review terkait penggunaan UPS apabila ditemukan perubahan suatu kondisi?	✓	

Tabel lampiran D. 63 Responden 5 (Lanjutan)

A.11.2.3	Keamanan kabel	1	Apakah penilaian risiko telah dilakukan atas lokasi kabel listrik dan kabel telekomunikasi atau jaringan?	✓	
		2	Apakah kabel listrik dan jaringan ditempatkan supaya terlindung dari gangguan, intersepsi, atau kerusakan?		✓
		3	Apakah penempatan kabel lstrik dan jaringan sudah terdokumentasi?		✓
		4	Apakah penentuan tempat kabel listrik dan jaringan sudah berdasarkan penilaian ancaman bencana alam dan ancaman pihak jahat?	✓	
		5	Apakah dilakukan review terkait penempatan posisi kabel dan ajaringan apabila ditemukan perubahan suatu kondisi?	✓	

A.11.2.4	Perawatan peralatan	1	Apakah terdapat jadwal perawatan peralatan yang ketat?		✓
		2	Apaakah perawatan peralatan diketahui oleh manajemen?		✓
		3	Apakah perawatan peralatan terdokumentasi?	✓	
		4	Apakah perawatan peralatan keamanan sudah sesuai dengan standar kemanan?		✓
		5	Apakah dilakukan review terkait terawatan keamanan apabila ditemukan perubahan suatu kondisi?	✓	
A.11.2.5	Penghapusan perangkat	1	Apakah terdapat proses yang mengontrol bagaimana perangkat dihapus dari daftar perangkat?	✓	
		2	Apakah proses kontol penghapusan perangkat dilakukan?		✓
		3	Apakah pemeriksaan langsung terhadap proses penghapusan perangkat dilakukan?		✓
		4	Apakah pengahapusan perangkat sudah disetujui oleh manajemen dan pimpinan?	✓	
		5	Apakah dilakukan review terkait penghapusan perangkat dari daftar peranghat apabila ditemukan perubahan suatu kondisi?		✓
A.11.2.6	Keamanan peralatan dan perangkat di luar lokasi	1	Apakah terdapat kebijakan yang mengatur keamanan perangkat di luar lokasi?		✓
		2	Apakah kebijakan perlindungan perangkat diluar lokasi (kantor) dikomunikasikan secara luas?		✓

Tabel lampiran D. 64 Responden 5 (Lanjutan)

		3	Apakah penempatan perlatan diluar lokasi terdokumentasi?	✓	
		4	Apakah penempatan perlatan diluar lokasi sudah memperhitungkan bahaya keamanan bencana alam atau ancaman prilaku jahat?	✓	
		5	Apakah dilakukan review terkait perlindungan peralatan diluar lokasi?	✓	
A.11.2.7	Pembuangan yang aman atau penggunaan kembali peralatan	1	Apakah terdapat kebijakan yang mengatur bagaimana perangkat informasi dapat digunakan kembali?	✓	
		2	Apakah mekanisme pengelolaan data, diverifikasi dengan benar sebelum digunakan kembali / dibuang?	✓	
		3	Apakah kebijakan penggunaan atau pembuanagan data sudah dikomunikasikan secara baik kepada karyawan?		✓

		4	Apakah pembuangan atau penggunaan kembali peralatan sudah berdasarkan pertimbangan keamanan?	✓	
		5	Apakah terdapat mekanisme review terkait penggunaan atau pembuangan apabila ditemukan perubahan suatu kondisi?	✓	
A.11.2.8	Peralatan pengguna tanpa pengawasan	1	Apakah organisasi memiliki kebijakan tentang bagaimana peralatan yang tidak dijaga harus dilindungi?		✓
		2	Apakah kontrol teknis diterapkan untuk mengamankan peralatan yang secara tidak sengaja ditinggalkan?		✓
		3	Apakah terdapat pendokumentasian terhadap barang - barang yang tidak sengaja ditinggalkan?		✓
		4	Apakah kebijakan terkait perlindungan perlatan yang tidak sengaja ditinggalkan sudah diketahui pimpinan dan manajemen?		✓
		5	Apakah dilakukan review terkait kebijakan perlindungan barang yang tdaik sengaja ditinggalkan?	✓	
A.11.2.9	Kebijakan *Clear desk and clear screen*	1	Apakah terdapat kebijakan *clear desk /clear screen?*	✓	
		2	Apakah kebijakan clear desk dan clear screen diberlakukan dengan baik?	✓	
		3	Apakah kebijakan terkait clear screen dan clear desk sudah dikomunikasikan dengan baik dengan karyawan?		✓

Tabel lampiran D. 65 Responden 5 (Lanjutan)

		4	Apakah kebijakan clear screen dan clear desk sudah sesuai dengan kebutuhan organisasi?	✓	
		5	Apakah dilakukan review terhadap kebijakan clear screen dan clear desk apabila ditemukan perubahan suatu kondisi?	✓	

Tabel lampiran D. 66 Responden 6

A.5	Kebijakan Keamanan Informasi		Pertanyaan	Ya	Tidak
A.5.1	Arahan manajemen untuk keamanan informasi				

A.5.1.1	Kebijakan untuk keamanan informasi	1	Apakah terdapat kebijakan keamanan informasi terkait pengelolaan informasi?	✓	
		2	Apakah kebijakan keamanan Informasi tersebut disetujui oleh manajemen dan pimpinan?	✓	
		3	Apakah kebijakan dikomunikasikan secara baik kepada karyawan?	✓	
		4	Apakah kebijakan dibuat sesuai dengan tujuan organisasi?		✓
		5	Apakah kebijakan dapat disesuaikan apabila ditemukan perubahan suatu kondisi?	✓	
A.5.1.2	Review kebijakan untuk keamanan informasi	1	Apakah dilakukan peninjauan terhadap kebijakan keamanan informasi?	✓	
		2	Apakah peninjauan dilakunan secara berkala?		✓
		3	Apakah peninjauan melibatkan manajemen dan pimpinan?		✓
		4	Apakah review dilakukan berdasarkan kebutuhan oraganisasi?	✓	
		5	Apakah dilakukan review terhadap kebijakan apabila ditemukan perubahan situasi?		✓
A.6	Keamanan Informasi Organisasi		Pertanyaan	Ya	Tidak
A.6.1	Internal Organisasi				

Tabel lampiran D. 67 Responden 6 (Lanjutan)

A.6.1.1	Peran dan tanggung jawab keamanan informasi	1	Apakah tanggung jawab terkait perlindungan perangkat pribadi, untuk melaksanakan proses keamanan, diidentifikasi, dan dikomunikasikan kepada pihak terkait?	✓	
		2	Apakah peran dan tanggungjawab telah sesuai dengan keahlian masing - masing karyawan?	✓	
		3	Apakah terdapat dokumentasi terkait pelaksanaan tugas dan tanggungjawab dalam menjaga informasi organisasi?		✓
		4	Apakah peran dan tanggungjawab karyawan sudah sesuai dengan tujuan organisasi?	✓	
		5	Apakah dilakuakan review terkait peran dan tanggungjawab karayawan dalam menjaga keamanan informasi organisasi?	✓	

A.6.1.2	Pemisahan tugas	1	Apakah tugas dan bidang tanggung jawab dipisahkan, untuk mengurangi peluang modifikasi yang tidak sah atau penyalahgunaan informasi, atau layanan?	✓□	
		2	Apakah pemisahan tugas sudah sesuai dengan keahlian masing - masing karyawan?		✓□
		3	Apakah pemisahan tugas sudah sesuai dengan kebijakan organisasi?		✓□
		4	Apakah pemisahan tugas, bidang dan tanggungajawab sudah sesuai dengan tujuan atau visi misi organisasi?		✓□
		5	Apakah pemisahan tugas, bidang dan tanggungjawab direview apabila ditemukan perubahan suatu kondisi?	✓□	
A.6.1.3	Kontak dengan pihak berwenang	1	Apakah terdapat prosedur yang mendokumentasikan kapan, dan oleh siapa, kontak dengan otoritas terkait akan dilakukan?		✓□
		2	Apakah kontak dengan otoritas terkait disetujui olem manajemen?		✓□
		3	Apakah terdapat proses yang merinci bagaimana dan kapan kontak perlu dilakukan?		✓□
		4	Apakah terdapat proses untuk kontak rutin dan berbagi pengetahuan?		✓□
		5	Apakah kontak dengan pihak terkait dilakukan secara rutin?	✓□	

Tabel lampiran D. 68 Responden 6 (Lanjutan)

A.6.1.4	Kontak dengan kelompok minat khusus	1	Apakah terdapat pihak yang berwenang untuk mengaktifkan keanggotaan?		✓□
		2	Apakah pengaktifan keanggotaan sudah dilakukan oleh pihak yang sesuai?		✓□
		3	Apakah pengaktifan keanggotaan sudah diketahui oleh manajemen dan pimpinan?		✓□
		4	Apakah pengaktifan keanggotaan sesuai atau sejalan dengan tujuan organiasasi?		✓□
		5	Apakah dilakukan review terkait pengaktifan keanggotaan apabila ditemukan perubahan suatu kondisi?	✓□	

A.6.1.5	Keamanan informasi dalam manajemen proyek	1	Apakah seluruh proyek sudah melalui beberapa penilaian keamanan informasi?		✓
		2	Apakah penilaian terkait keamanan informasi sudah mengacu pada suatu standar?	✓	
		3	Apakah penilaian keamanan informasi terdokumentasi?	✓	
		4	Apakah penilaian keamanan informasi sesuai dengan tujuan organisasi?	✓	
		5	Apakah penilaian keamanan informasi pada suatu proyek dilakukan secara rutin sesuai tahapan proyek?	✓	
A.6.2	Perangkat Seluler dan *Teleworking*		Pertanyaan	Ya	Tidak
A.6.2.1	Kebijakan perangkat seluler	1	Apakah terdapat kebijakan terkait perangkat seluler?		✓
		2	Apakah kebijakan terkait perangkat selular mendapat persetujuan manajemen?		✓
		3	Apakah terdapat kebijakan yang mendokumentasikan dan menangani risiko dari penggunaan perangkat seluler (penggunaan hotspot ilegal)?		✓
		4	Apakah kebijakan terkait perangkat selular sesuai dengan tujuan organisasi?		✓
		5	Apakah kebijakan terkait perangkat seluler direview apabila ditemukan perubahan pada suatu kondisi?	✓	

Tabel lampiran D. 69 Responden 6 (Lanjutan)

A.6.2.2	*Teleworking*	1	Apakah terdapat kebijakan untuk *teleworking* (kerja diluar kantor) misalnya kerja dari rumah (WFH)?	✓	
		3	Apakah terdapat mekanisme atau proses yang ditetapkan bagi pekerja jarak jauh untuk mendapatkan akses (terhadap layanan/sistem)?	✓	
		4	Apakah karyawan yang akan melakukan WFH diberi pengarahan terkait perlindungan perangkat yang mereka gunakan?		✓
		5	Apakah dilakukan review terkait kebijakan WFH apabila ditemukan perubahan suatu kondisi?	✓	
A.9	Kontrol akses		Pertanyaan	Ya	Tidak
A.9.1	Persyaratan bisnis untuk kontrol akses				

A.9.1.1	Kebijakan kontrol akses	1	Apakah terdapat kebijakan kontrol akses?	✓	
		2	Apakah terdapat kebijakan terkait kontrol akses berdasarkan kebutuhan proses bisnis?	✓	
		3	Apakah kebijakan terkait kontrol akses dikomunikasikan dengan baik dengan manajemen?		✓
		4	Apakah kebijakan terkait kontrol akses sudah sesuai dengan tujuan organisasi?		✓
		5	Apakah kebijakan terkait kontrol akses di review apabila ditemukan perubahan pada suatu kondisi?	✓	
A.9.1.2	Akses ke jaringan dan layanan jaringan	1	Apakah terdapat kontrol untuk memastikan pengguna hanya memiliki akses ke jaringan khusus yang diperlukan untuk tugas mereka	✓	
		2	Apakah kontrol pengguna pada suatu jaringan sudah disetujui manajemen?	✓	
		3	Apakah layanan jaringan sudah dikomunikasikan secara baik kepada pihak terkait?		✓
		4	Apakah layanan jaringan yang didapatkan pengguna sudah mengacu pada suatu standar?	✓	
		5	Apakah dilakukan perubahan layanan terkait akses jaringan apabila ditemukan perubahan suatu kondisi?	✓	
A.9.2	Manajemen akses pengguna		Pertanyaan	Ya	Tidak

Tabel lampiran D. 70 Responden 6 (Lanjutan)

A.9.2.1	Pendaftaran pengguna dan pencabutan pendaftaran	1	Apakah terdapat proses pendaftaran akses untuk pengguna secara formal?	✓	
		2	Apakah proses pendaftaran akses untuk pengguna sudah disetujui oleh manajemen?	✓	
		3	Apakah proses pendaftaran akses untuk pengguna sudah terdokumentasi?		✓
		4	Apakah pemberian akses untuk pengguna sudah sesuai dengan tujuan organisasi?	✓	
		5	Apakah akses unntuk pengguna direview apabila ditemukan perubahan suatu kondisi?	✓	

A.9.2.2	Penyediaan akses pengguna	1	Apakah terdapat proses penyediaan akses bagi pengguna untuk menetapkan hak akses semua jenis dan layanan?	✓	
		2	Apakah proses penyediaan akases bagi pengguna sudah disetujui oleh manajemen?	✓	
		3	Apakah penyediaan akses untuk pengguna sudah terdokumentasi?		✓
		4	Apakah penyediaan akses untuk pengguna sudah sesuai dengan tujuan organisasi?		✓
		5	Apakah dilakukan review terkait penyediaan akses untuk pengguna apabila ditemukan perubahan suatu kondisi?	✓	
A.9.2.3	Pengelolaan hak akses istimewa	1	Apakah akun dengan akses istimewa (admin dan super admin) dikelola dan dikontrol secara terpisah?	✓	
		2	Apakah pengelolaan akses super admin dan super admin mengacu pada suatu standar keamanan?	✓	
		3	Apakah pengelolaan akun admin dan super admin sudah terdokumentasi?	✓	
		4	Apakah pengelolaan akun admin dan super admin sudah sesuai dengan tujuan organisasi?		✓
		5	Apakah dilakukan review terkait pengelolaan akun admin dan superadmin apabila ditemukan perubahan suatu kondisi?	✓	

Tabel lampiran D. 71 Responden 6 (Lanjutan)

A.9.2.4	Pengelolaan informasi otentikasi rahasia pengguna	1	Apakah terdapat proses manajemen secara formal untuk mengontrol informasi rahasia?	✓	
		2	Apakah pengelolaan informasi rahasia pengguna sudah mengacu pada suatu standar keamanan?		✓
		3	Apakah mekanisme pengelolaan data rahasia pengguna telah dikomunikasikan secara baik kepada seluruh karyawan terkait?		✓
		4	Apakah proses pengelolaan data rahasia pengguna diketahui oleh manajemen?		✓

		5	Apak dialakukan review terkait pengelolaan data rahasia pengguna apabila ditemukan perubahan kondisi?	✓□	
A.9.2.5	Review hak akses pengguna	1	Apakah terdapat proses bagi pemilik perangkat untuk meninjau hak akses ke perangkat mereka secara teratur?		✓□
		2	Apakah proses tinjauan ini diverifikasi?		✓□
		3	ApaKah proses review terdokumentasi?		✓□
		4	Apakah proses review terkait hak akses pengguna mendapat persetujuan manajemen?		✓□
		5	Apakah proses review sudah sesuai dengan tujuan organisasi?	✓□	
A.9.2.6	Penghapusan atau penyesuaian hak akses	1	Apakah terdapat mekanisme dan proses untuk memastikan hak akses pengguna dihapus saat pemutusan hubungan kerja, atau saat perubahan peran?	✓□	
		2	Apakah proses untuk penghapusan hak akses sudah diketahui oleh manajemen?		✓□
		3	Apakah proses penghapusan kah akses terdokumentasi?		✓□
		4	Apakah proses penghapusan dan penyesuaian hak akses sudah sesuai dengan tujuan oraganisasi?	✓□	
		5	Apakah dilakukan review terkait proses penghapusan dan penyesuaian hak akses apabila ditemukan perubahan suatu kondisi?	✓□	
A.9.3	Tanggung jawab pengguna		Pertanyaan	Ya	Tidak

Tabel lampiran D. 72 Responden 6 (Lanjutan)

A.9.3.1	Penggunaan informasi otentikasi rahasia	1	Apakah terdapat dokumen kebijakan yang mencakup praktik organisasi tentang bagaimana informasi otentikasi rahasia harus ditangani?		✓□
		2	Dokumen tersebut dikomunikasikan kepada semua pengguna		✓□
		3	Apakah dokumen tersebut mengacu pada sebuah standar keamanan?		✓□
		4	Apakah penanganan informasi rahasia sudah sesuai denagan tujuan organisasi?	✓□	

		5	Apakah dilakukan review terhadap dokumen yang berisi tentang penanganan informasi rahasia pengguna apabila ditemukan perubahan suatu kondisi?	✓□	
A.9.4	Kontrol akses sistem dan aplikasi		Pertanyaan	Ya	Tidak
A.9.4.1	Pembatasan akses informasi	1	Apakah akses terhadap informasi dan fungsi sistem aplikasi dibatasi sesuai dengan kebijakan kontrol akses?	✓□	
		2	Apakah pembatasan akses terhadap informasi dan fungsi aplikasi disetujui oleh manajemen?		✓□
		3	Apakah pembatasan akses terhadap inforamasi dan fungsi aplikasi sudah dikomunikasikan kepada seluruh karyawan?	✓□	
		4	Apakah pembatasan akses terhadap inforamasi dan fungsi aplikasi sesuai dengan tujuan organisasi?	✓□	
		5	Apakah dilakuakan review terkait pembatasan informasi dan fungsi apalikasi apabila ditemukan perubahan suatu kondisi?	✓□	
A.9.4.2	Amankan prosedur log-on	1	Apakah akses dikontrol oleh prosedur log-on yang aman?	✓□	
		2	Apaakah prosesudh log-on sudah mengacu pada suatu standar keamanan?		✓□
		3	Apakah terdapat mekanisme yang mendokumentasikan prosedur log-on?		✓□
		4	apakah prosedur log-on dirancang agar terhindar dari gangguan pihak jahat?	✓□	
		5	Apakah terdapat mekanisme review terkait keamanan prosedur log-on apabila dietemukan isu atau perubahan suatu kondisi?	✓□	

Tabel lampiran D. 73 Responden 6 (Lanjutan)

A.9.4.3	Sistem manajemen kata sandi	1	Apakah sistem kata sandi bersifat interaktif?		✓□
		2	Apakah diperlukan kata sandi yang rumit?		✓□
		3	Apakah manajemen kata sandi sudah mengacu pada suatu standar keamanan?		✓□
		4	Apakah terdapat kewajiban untuk mengganti kata sandi secara rutin?	✓□	
		5	Apakah manajemen pengelolaan kata sandi direview apabila ditemukan perubahan suatu kondisi?	✓□	

A.9.4.4	Penggunaan program utilitas dengan hak istimewa	1	Apakah program utilitas hak istimewa dibatasi dan dipantau?		✓
		2	Apakah penggunaan program utilitas dengan hak istimewa sudah disetujui oleh manajemen?	✓	
		3	Apakah penggunaan program utilitas dengan hak istimewa sudah terdokumentasi?	✓	
		4	Apakah penggunaan program utilitas dengan hak istimewa sudah sesuai dengan kebijakan dan tujuan organisasi?		✓
		5	Apakah dilakuna review terkait penggunaan program utilitas dengan hak akses istimewa apabila ditemukan perubahan suatu kondisi?	✓	
A.9.4.5	Kontrol akses ke kode sumber program	1	Apakah akses terhadap kode sumber *(Source Code)* sistem dilindungi oleh kontrol akses?	✓	
		2	Apakah perlindungan terhadap source code disetujui oleh manajemen?		✓
		3	Apakah perlindungan terhadap source code di komunikasikan terhadap seluruh karyawan terkait?		✓
		4	Apakah perlindungan terhadap source code sudah sesuai dengan tujuan dan arahan organisasi?		✓
		5	Apakah dilakukan review terkait perlindungan source code apabila ditemukan perubahan suatu kondisi?	✓	
A.11	Keamanan fisik dan lingkungan		Pertanyaan	Ya	Tidak
A.11.1	Area aman				
A.11.1.1	Perimeter (pembatas) keamanan fisik	1	Apakah terdapat perimeter (pembatas) keamanan khusus?	✓	

Tabel lampiran D. 74 Responden 6 (Lanjutan)

		2	Apakah area informasi sensitif atau kritis dipisahkan dan dikontrol dengan baik?	✓	
		3	Apakah pembatas keamanan fisik sudah sesuai berdasarkan standar keamanan?	✓	
		4	Apakah pembatas keamanan fisik dirancang untuk perlindungan terhadap ancaman kejahatan?	✓	

		5	Apakah pembatas fisik dievaluasti apabila ditemukan perubahan kondisi?	✓	
A.11.1.2	Kontrol entri fisik	1	Apakah area aman *(secure area)* memiliki sistem kontrol masuk yang sesuai untuk memastikan hanya personel yang berwenang yang memiliki akses?	✓	
		2	Apakah secure area telah mengikuti standar keamanan?	✓	
		3	Apakah kontrol entri sudah sesuai dengan kebijakan organisaisi?		✓
		4	Apakah personel yang dapat masuk ke secure area sudah sesuai dengan kebijakan organisasi?		✓
		5	Apakah kontrol entri terhadap secure area direview apabila ditemukan perubahan terhadap suatu kondisi?	✓	
A.11.1.3	Mengamankan kantor, kamar, dan fasilitas	1	Apakah ruangan kantor dan fasilitas lain telah dirancang dan dikonfigurasi dengan mempertimbangkan keamanan?		✓
		2	Apakah terdapat proses untuk menjaga keamanan (misalnya mengunci, membersihkan meja, dll.)?	✓	
		3	Apak terkait keamanan ruangan sudah dikomunikasikan dengan baik kepada karayawan?		✓
		4	apakah ruangan kantor sudah sesuai dengan suatu standar?	✓	
		5	Apakah dilakuna review terhadap keamanan kantor atau ruangan apabila ditemukan perubahan suatu kondisi?	✓	
A.11.1.4	Melindungi dari ancaman eksternal dan lingkungan	1	Apakah perlindungan fisik untuk mencegah bencana alam, serangan jahat atau kecelakaan telah dirancang?		✓

Tabel lampiran D. 75 Responden 6 (Lanjutan)

		2	Apakah perlindungan fisik terkait ancaman bencana alam atau serangan jahat sudah disetujui oleh manajemen?	✓	
		3	Apakah perlindungan fisik sudah terdukomentasi?		✓
		4	Apakah perlindungan fisik terkait ancaman bencana alam dan pihak jahat sudah sesuai standar keamanan?	✓	

		5	Apakah dilakukan review terkait rancanagan perlindungan fisik apabila ditemukan perubahan suatu kondisi?	✓	
A.11.1.5	Bekerja di tempat yang aman	1	Apakah terdapat area aman *(Secure Area)?*	✓	
		2	Apakah s*ecure area* memiliki kebijakan dan proses yang sesuai?		✓
		3	Apakah kebijakan dan proses dilakukan dan dipantau?		✓
		4	Apakah secure area sudah distujui organisasi?	✓	
		5	Apakah dilakukan review terkait secure area apabila ditemukan perubahan pada suatu kondisi?	✓	
A.11.1.6	Area pengiriman dan pemuatan	1	Apakah terdapat area pengiriman / pemuatan yang terpisah?	✓	
		2	Apakah akses ke area pengiriman/pemuatan dikendalikan?		✓
		3	Apakah akses area pemuatan diisolasi dari fasilitas pemrosesan informasi?	✓	
		4	Apakah secure area sudah distujui organisasi?	✓	
		5	Apakah dilakukan review terkait secure area apabila ditemukan perubahan pada suatu kondisi?	✓	
A.11.2	Peralatan		Pertanyaan	Ya	Tidak
A.11.2.1	Penempatan dan perlindungan peralatan	1	Apakah bahaya lingkungan diidentifikasi dan dipertimbangkan ketika lokasi peralatan dipilih?	✓	
		2	Apakah risiko akses yang tidak sah telah dipertimbangkan saat menentukan lokasi peralatan?		✓
		3	Apakah penempatan peralatan sudah terdokumentasi?	✓	
		4	Apakah penempatan peralatan sudah seuasuai dengan kebutuhan organisasi?	✓	

Tabel lampiran D. 76 Responden 6 (Lanjutan)

		5	Apaha dilakukan review terkait penempatan dan perlindungan peralatan apabila ditemukan perubahan suatu kondisi?	✓	
A.11.2.2	Utilitas pendukung	1	Apakah terdapat UPS atau generator cadangan?	✓	
		2	Apakah sistem UPS sudah diuji dalam skala waktu yang sesuai?	✓	
		3	Apakah UPS yangdigunakan sudah berdasarkan suatu standar?	✓	

		4	Apakah penggunaan UPS sudah berdasarkan kebutuhan organisasi?		✓
		5	Apakah terdapat mekanisme review terkait penggunaan UPS apabila ditemukan perubahan suatu kondisi?	✓	
A.11.2.3	Keamanan kabel	1	Apakah penilaian risiko telah dilakukan atas lokasi kabel listrik dan kabel telekomunikasi atau jaringan?	✓	
		2	Apakah kabel listrik dan jaringan ditempatkan supaya terlindung dari gangguan, intersepsi, atau kerusakan?	✓	
		3	Apakah penempatan kabel lstrik dan jaringan sudah terdokumentasi?		✓
		4	Apakah penentuan tempat kabel listrik dan jaringan sudah berdasarkan penilaian ancaman bencana alam dan ancaman pihak jahat?		✓
		5	Apakah dilakukan review terkait penempatan posisi kabel dan ajaringan apabila ditemukan perubahan suatu kondisi?	✓	
A.11.2.4	Perawatan peralatan	1	Apakah terdapat jadwal perawatan peralatan yang ketat?		✓
		2	Apakah perawatan peralatan diketahui oleh manajemen?		✓
		3	Apakah perawatan peralatan terdokumentasi?		✓
		4	Apakah perawatan peralatan keamanan sudah sesuai dengan standar kemanan?		✓
		5	Apakah dilakukan review terkait terawatan keamanan apabila ditemukan perubahan suatu kondisi?	✓	
A.11.2.5	Penghapusan perangkat	1	Apakah terdapat proses yang mengontrol bagaimana perangkat dihapus dari daftar perangkat?	✓	
		2	Apakah proses kontol penghapusan perangkat dilakukan?	✓	

Tabel lampiran D. 77 Responden 6 (Lanjutan)

		3	Apakah pemeriksaan langsung terhadap proses penghapusan perangkat dilakukan?	✓	
		4	Apakah pengahapusan perangkat sudah disetujui oleh manajemen dan pimpinan?		✓
		5	Apakah dilakukan review terkait penghapusan perangkat dari daftar peranghat apabila ditemukan perubahan suatu kondisi?	✓	
A.11.2.6	Keamanan peralatan dan perangkat di luar lokasi	1	Apakah terdapat kebijakan yang mengatur keamanan perangkat di luar lokasi?	✓	

		2	Apakah kebijakan perlindungan perangkat diluar lokasi (kantor) dikomunikasikan secara luas?		✓□
		3	Apakah penempatan perlatan diluar lokasi terdokumentasi?		✓□
		4	Apakah penempatan perlatan diluar lokasi sudah memperhitungkan bahaya keamanan bencana alam atau ancaman prilaku jahat?	✓□	
		5	Apakah dilakukan review terkait perlindungan peralatan diluar lokasi?	✓□	
A.11.2.7	Pembuangan yang aman atau penggunaan kembali peralatan	1	Apakah terdapat kebijakan yang mengatur bagaimana perangkat informasi dapat digunakan kembali?	✓□	
		2	Apakah mekanisme pengelolaan data, diverifikasi dengan benar sebelum digunakan kembali / dibuang?		✓□
		3	Apakah kebijakan penggunaan atau pembuanagan data sudah dikomunikasikan secara baik kepada karyawan?		✓□
		4	Apakah pembuangan atau penggunaan kembali peralatan sudah berdasarkan pertimbangan keamanan?	✓□	
		5	Apakah terdapat mekanisme review terkait penggunaan atau pembuangan apabila ditemukan perubahan suatu kondisi?	✓□	
A.11.2.8	Peralatan pengguna tanpa pengawasan	1	Apakah organisasi memiliki kebijakan tentang bagaimana peralatan yang tidak dijaga harus dilindungi?	✓□	
		2	Apakah kontrol teknis diterapkan untuk mengamankan peralatan yang secara tidak sengaja ditinggalkan?		✓□

Tabel lampiran D. 78 Responden 6 (Lanjutan)

		3	Apakah terdapat pendokumentasian terhadap barang - barang yang tidak sengaja ditinggalkan?	✓□	
		4	Apakah kebijakan terkait perlindungan perlatan yang tidak sengaja ditinggalkan sudah diketahui pimpinan dan manajemen?		✓□
		5	Apakah dilakukan review terkait kebijakan perlindungan barang yang tdaik sengaja ditinggalkan?		✓□
A.11.2.9	Kebijakan *Clear desk and clear screen*	1	Apakah terdapat kebijakan *clear desk /clear screen?*	✓□	

		2	Apakah kebijakan clear desk dan clear screen diberlakukan dengan baik?	✓	
		3	Apakah kebijakan terkait clear screen dan clear desk sudah dikomunikasikan dengan baik dengan karyawan?		✓
		4	Apakah kebijakan clear screen dan clear desk sudah sesuai dengan kebutuhan organisasi?		✓
		5	Apakah dilakukan review terhadap kebijakan clear screen dan clear desk apabila ditemukan perubahan suatu kondisi?	✓	

Tabel lampiran D. 79 Responden 7

A.5	Kebijakan Keamanan Informasi		Pertanyaan	Ya	Tidak
A.5.1	Arahan manajemen untuk keamanan informasi				
A.5.1.1	Kebijakan untuk keamanan informasi	1	Apakah terdapat kebijakan keamanan informasi terkait pengelolaan informasi?	✓	
		2	Apakah kebijakan keamanan informasi tersebut disetujui oleh manajemen dan pimpinan?		✓
		3	Apakah kebijakan dikomunikasikan secara baik kepada karyawan?		✓
		4	Apakah kebijakan dibuat sesuai dengan tujuan organisasi?	✓	

Tabel lampiran D. 80 Responden 7 (Lanjutan)

		5	Apakah kebijakan dapat disesuaikan apabila ditemukan perubahan suatu kondisi?	✓	
A.5.1.2	Review kebijakan untuk keamanan informasi	1	Apakah dilakukan peninjauan terhadap kebijakan keamanan informasi?	✓	
		2	Apakah peninjauan dilakunan secara berkala?		✓
		3	Apakah peninjauan melibatkan manajemen dan pimpinan?		✓
		4	Apakah review dilakukan berdasarkan kebutuhan oraganisasi?	✓	

		5	Apakah dilakukan review terhadap kebijakan apabila ditemukan perubahan situasi?		✓□
A.6	Keamanan Informasi Organisasi		Pertanyaan	Ya	Tidak
A.6.1	Internal Organisasi				
A.6.1.1	Peran dan tanggung jawab keamanan informasi	1	Apakah tanggung jawab terkait perlindungan perangkat pribadi, untuk melaksanakan proses keamanan, diidentifikasi, dan dikomunikasikan kepada pihak terkait?	✓□	
		2	Apakah peran dan tanggungjawab telah sesuai dengan keahlian masing - masing karyawan?	✓□	
		3	Apakah terdapat dokumentasi terkait pelaksanaan tugas dan tanggungjawab dalam menjaga informasi organisasi?		✓□
		4	Apakah peran dan tanggungjawab karyawan sudah sesuai dengan tujuan organisasi?	✓□	
		5	Apakah dilakuakan review terkait peran dan tanggungjawab karayawan dalam menjaga keamanan informasi organisasi?	✓□	
A.6.1.2	Pemisahan tugas	1	Apakah tugas dan bidang tanggung jawab dipisahkan, untuk mengurangi peluang modifikasi yang tidak sah atau penyalahgunaan informasi, atau layanan?	✓□	
		2	Apakah pemisahan tugas sudah sesuai dengan keahlian masing - masing karyawan?	✓□	
		3	Apakah pemisahan tugas sudah sesuai dengan kebijakan organisasi?		✓□

Tabel lampiran D. 81 Responden 7 (Lanjutan)

		4	Apakah pemisahan tugas, bidang dan tanggungajawab sudah sesuai dengan tujuan atau visi misi organisasi?	✓□	
		5	Apakah pemisahan tugas, bidang dan tanggungjawab direview apabila ditemukan perubahan suatu kondisi?	✓□	
A.6.1.3	Kontak dengan pihak berwenang	1	Apakah terdapat prosedur yang mendokumentasikan kapan, dan oleh siapa, kontak dengan otoritas terkait akan dilakukan?		✓□
		2	Apakah kontak dengan otoritas terkait disetujui oleh manajemen?	✓□	

		3	Apakah terdapat proses yang merinci bagaimana dan kapan kontak perlu dilakukan?	✓	
		4	Apakah terdapat proses untuk kontak rutin dan berbagi pengetahuan?		✓
		5	Apakah kontak dengan pihak terkait dilakukan secara rutin?		✓
A.6.1.4	Kontak dengan kelompok minat khusus	1	Apakah terdapat pihak yang berwenang untuk mengaktifkan keanggotaan?		✓
		2	Apakah pengaktifan keanggotaan sudah dilakukan oleh pihak yang sesuai?		✓
		3	Apakah pengaktifan keanggotaan sudah diketahui oleh manajemen dan pimpinan?		✓
		4	Apakah pengaktifan keanggotaan sesuai atau sejalan dengan tujuan organiasasi?		✓
		5	Apakah dilakukan review terkait pengaktifan keanggotaan apabila ditemukan perubahan suatu kondisi?	✓	
A.6.1.5	Keamanan informasi dalam manajemen proyek	1	Apakah seluruh proyek sudah melalui beberapa penilaian keamanan informasi?	✓	
		2	Apakah penilaian terkait keamanan informasi sudah mengacu pada suatu standar?	✓	
		3	Apakah penilaian keamanan informasi terdokumentasi?	✓	
		4	Apakah penilaian keamanan informasi sesuai dengan tujuan organisasi?		✓
		5	Apakah penilaian keamanan informasi pada suatu proyek dilakukan secara rutin sesuai tahapan proyek?	✓	

Tabel lampiran D. 82 Responden 7 (Lanjutan)

A.6.2	Perangkat Seluler dan *Teleworking*		Pertanyaan	Ya	Tidak
A.6.2.1	Kebijakan perangkat seluler	1	Apakah terdapat kebijakan terkait perangkat seluler?	✓	
		2	Apakah kebijakan terkait perangkat selular mendapat persetujuan manajemen?		✓
		3	Apakah terdapat kebijakan yang mendokumentasikan dan menangani risiko dari penggunaan perangkat seluler (penggunaan hotspot ilegal)?	✓	
		4	Apakah kebijakan terkait perangkat selular sesuai dengan tujuan organisasi?		✓

		5	Apakah kebijakan terkait perangkat seluler *direview* apabila ditemukan perubahan pada suatu kondisi?	✓	
A.6.2.2	*Teleworking*	1	Apakah terdapat kebijakan untuk *teleworking* (kerja diluar kantor) misalnya kerja dari rumah (WFH)?	✓	
		2	Apakah *teleworking* mendapat persetujuan manajemen?		✓
		3	Apakah terdapat mekanisme atau proses yang ditetapkan bagi pekerja jarak jauh untuk mendapatkan akses (terhadap layanan/sistem)?	✓	
		4	Apakah karyawan yang akan melakukan WFH diberi pengarahan terkait perlindungan perangkat yang mereka gunakan?		✓
		5	Apakah dilakukan *review* terkait kebijakan WFH apabila ditemukan perubahan suatu kondisi?	✓	
A.9	Kontrol akses		Pertanyaan	Ya	Tidak
A.9.1	Persyaratan bisnis untuk kontrol akses				
A.9.1.1	Kebijakan kontrol akses	1	Apakah terdapat kebijakan kontrol akses?	✓	
		2	Apakah terdapat kebijakan terkait kontrol akses berdasarkan kebutuhan proses bisnis?	✓	
		3	Apakah kebijakan terkait kontrol akses dikomunikasikan dengan baik dengan manajemen?		✓
		4	Apakah kebijakan terkait kontrol akses sudah sesuai dengan tujuan organisasi?	✓	

Tabel lampiran D. 83 Responden 7 (Lanjutan)

		5	Apakah kebijakan terkait kontrol akses di *review* apabila ditemukan perubahan pada suatu kondisi?	✓	
A.9.1.2	Akses ke jaringan dan layanan jaringan	1	Apakah terdapat kontrol untuk memastikan pengguna hanya memiliki akses ke jaringan khusus yang diperlukan untuk tugas mereka	✓	
		2	Apakah kontrol pengguna pada suatu jaringan sudah disetujui manajemen?		✓
		3	Apakah layanan jaringan sudah dikomunikasikan secara baik kepada pihak terkait?		✓

		4	Apakah layanan jaringan yang didapatkan pengguna sudah mengacu pada suatu standar?		✓
		5	Apakah dilakukan perubahan layanan terkait akses jaringan apabila ditemukan perubahan suatu kondisi?	✓	
A.9.2	Manajemen akses pengguna		Pertanyaan	Ya	Tidak
A.9.2.1	Pendaftaran pengguna dan pencabutan pendaftaran	1	Apakah terdapat proses pendaftaran akses untuk pengguna secara formal?	✓	
		2	Apakah proses pendaftaran akses untuk pengguna sudah disetujui oleh manajemen?	✓	
		3	Apakah proses pendaftaran akses untuk pengguna sudah terdokumentasi?	✓	
		4	Apakah pemberian akses untuk pengguna sudah sesuai dengan tujuan organisasi?	✓	
		5	Apakah akses unntuk pengguna *direview* apabila ditemukan perubahan suatu kondisi?	✓	
A.9.2.2	Penyediaan akses pengguna	1	Apakah terdapat proses penyediaan akses bagi pengguna untuk menetapkan hak akses semua jenis dan layanan?	✓	
		2	Apakah proses penyediaan akases bagi pengguna sudah disetujui oleh manajemen?	✓	
		3	Apakah penyediaan akses untuk pengguna sudah terdokumentasi?		✓

Tabel lampiran D. 84 Responden 7 (Lanjutan)

		4	Apakah penyediaan akses untuk pengguna sudah sesuai dengan tujuan organisasi?	✓	
		5	Apakah dilakukan *review* terkait penyediaan akses untuk pengguna apabila ditemukan perubahan suatu kondisi?	✓	
A.9.2.3	Pengelolaan hak akses istimewa	1	Apakah akun dengan akses istimewa (admin dan super admin) dikelola dan dikontrol secara terpisah?	✓	
		2	Apakah pengelolaan akses super admin dan super admin mengacu pada suatu standar keamanan?		✓

		3	Apakah pengelolaan akun admin dan super admin sudah terdokumentasi?		✓
		4	Apakah pengelolaan akun admin dan super admin sudah sesuai dengan tujuan organisasi?	✓	
		5	Apakah dilakukan *review* terkait pengelolaan akun admin dan superadmin apabila ditemukan perubahan suatu kondisi?	✓	
A.9.2.4	Pengelolaan informasi otentikasi rahasia pengguna	1	Apakah terdapat proses manajemen secara formal untuk mengontrol informasi rahasia?		✓
		2	Apakah pengelolaan informasi rahasia pengguna sudah mengacu pada suatu standar keamanan?		✓
		3	Apakah mekanisme pengelolaan data rahasia pengguna telah dikomunikasikan secara baik kepada seluruh karyawan terkait?		✓
		4	Apakah proses pengelolaan data rahasia pengguna diketahui oleh manajemen?		✓
		5	Apak dialakukan *review* terkait pengelolaan data rahasia pengguna apabila ditemukan perubahan kondisi?	✓	
A.9.2.5	*Review* hak akses pengguna	1	Apakah terdapat proses bagi pemilik perangkat untuk meninjau hak akses ke perangkat mereka secara teratur?	✓	
		2	Apakah proses tinjauan ini diverifikasi?		✓
		3	Apakah proses *review* terdokumentasi?		✓

Tabel lampiran D. 85 Responden 7 (Lanjutan)

		4	Apakah proses *review* terkait hak akses pengguna mendapat persetujuan manajemen?		✓
		5	Apakah proses *review* sudah sesuai dengan tujuan organisasi?	✓	
A.9.2.6	Penghapusan atau penyesuaian hak akses	1	Apakah terdapat mekanisme dan proses untuk memastikan hak akses pengguna dihapus saat pemutusan hubungan kerja, atau saat perubahan peran?	✓	
		2	Apakah proses untuk penghapusan hak akses sudah diketahui oleh manajemen?	✓	

		3	Apakah proses penghapusan kah akses terdokumentasi?		✓
		4	Apakah proses penghapusan dan penyesuaian hak akses sudah sesuai dengan tujuan oraganisasi?	✓	
		5	Apakah dilakukan *review* terkait proses penghapusan dan penyesuaian hak akses apabila ditemukan perubahan suatu kondisi?	✓	
A.9.3	Tanggung jawab pengguna		Pertanyaan	Ya	Tidak
A.9.3.1	Penggunaan informasi otentikasi rahasia	1	Apakah terdapat dokumen kebijakan yang mencakup praktik organisasi tentang bagaimana informasi otentikasi rahasia harus ditangani?	✓	
		2	Dokumen tersebut dikomunikasikan kepada semua pengguna	✓	
		3	Apakah dokumen tersebut mengacu pada sebuah standar keamanan?		✓
		4	Apakah penanganan informasi rahasia sudah sesuai denagan tujuan organisasi?		✓
		5	Apakah dilakukan *review* terhadap dokumen yang berisi tentang penanganan informasi rahasia pengguna apabila ditemukan perubahan suatu kondisi?	✓	
A.9.4	Kontrol akses sistem dan aplikasi		Pertanyaan	Ya	Tidak
A.9.4.1	Pembatasan akses informasi	1	Apakah akses terhadap informasi dan fungsi sistem aplikasi dibatasi sesuai dengan kebijakan kontrol akses?	✓	
		2	Apakah pembatasan akses terhadap informasi dan fungsi aplikasi disetujui oleh manajemen?	✓	

Tabel lampiran D. 86 Responden 7 (Lanjutan)

		3	Apakah pembatasan akses terhadap inforamasi dan fungsi aplikasi sudah dikomunikasikan kepada seluruh karyawan?		✓
		4	Apakah pembatasan akses terhadap inforamasi dan fungsi aplikasi sesuai dengan tujuan organisasi?		✓
		5	Apakah dilakuakan *review* terkait pembatasan informasi dan fungsi apalikasi apabila ditemukan perubahan suatu kondisi?	✓	
A.9.4.2	Amankan prosedur log-on	1	Apakah akses dikontrol oleh prosedur log-on yang aman?	✓	

		2	Apaakah prosedur log-on sudah mengacu pada suatu standar keamanan?		✓□
		3	Apakah terdapat mekanisme yang mendokumentasikan prosedur log-on?	✓□	
		4	apakah prosedur log-on dirancang agar terhindar dari gangguan pihak jahat?	✓□	
		5	Apakah terdapat mekanisme *review* terkait keamanan prosedur log-on apabila dietemukan isu atau perubahan suatu kondisi?	✓□	
A.9.4.3	Sistem manajemen kata sandi	1	Apakah sistem kata sandi bersifat interaktif?		✓□
		2	Apakah diperlukan kata sandi yang rumit?	✓□	
		3	Apakah manajemen kata sandi sudah mengacu pada suatu standar keamanan?	✓□	
		4	Apakah terdapat kewajiban untuk mengganti kata sandi secara rutin?		✓□
		5	Apakah manajemen pengelolaan kata sandi *direview* apabila ditemukan perubahan suatu kondisi?	✓□	
A.9.4.4	Penggunaan program utilitas dengan hak istimewa	1	Apakah program utilitas hak istimewa dibatasi dan dipantau?	✓□	
		2	Apakah penggunaan program utilitas dengan hak istimewa sudah disetujui oleh manajemen?	✓□	
		3	Apakah penggunaan program utilitas dengan hak istimewa sudah terdokumentasi?		✓□

Tabel lampiran D. 87 Responden 7 (Lanjutan)

		4	Apakah penggunaan program utilitas dengan hak istimewa sudah sesuai dengan kebijakan dan tujuan organisasi?	✓□	
		5	Apakah dilakuna *review* terkait penggunaan program utilitas dengan hak akses istimewa apabila ditemukan perubahan suatu kondisi?	✓□	
A.9.4.5	Kontrol akses ke kode sumber program	1	Apakah akses terhadap kode sumber *(Source Code)* sistem dilindungi oleh kontrol akses?	✓□	
		2	Apakah perlindungan terhadap source code disetujui oleh manajemen?		✓□

		3	Apakah perlindungan terhadap source code di komunikasikan terhadap seluruh karyawan terkait?	✓	
		4	Apakah perlindungan terhadap source code sudah sesuai dengan tujuan dan arahan organisasi?	✓	
		5	Apakah dilakukan *review* terkait perlindungan source code apabila ditemukan perubahan suatu kondisi?	✓	
A.11	Keamanan fisik dan lingkungan		Pertanyaan	Ya	Tidak
A.11.1	Area aman				
A.11.1.1	Perimeter (pembatas) keamanan fisik	1	Apakah terdapat perimeter (pembatas) keamanan khusus?	✓	
		2	Apakah area informasi sensitif atau kritis dipisahkan dan dikontrol dengan baik?	✓	
		3	Apakah pembatas keamanan fisik sudah sesuai berdasarkan standar keamanan?		✓
		4	Apakah pembatas keamanan fisik dirancang untuk perlindungan terhadap ancaman kejahatan?	✓	
		5	Apakah pembatas fisik dievaluasti apabila ditemukan perubahan kondisi?	✓	
A.11.1.2	Kontrol entri fisik	1	Apakah area aman *(secure area)* memiliki sistem kontrol masuk yang sesuai untuk memastikan hanya personel yang berwenang yang memiliki akses?	✓	
		2	Apakah secure area telah mengikuti standar keamanan?	✓	
		3	Apakah kontrol entri sudah sesuai dengan kebijakan organisaisi?	✓	

Tabel lampiran D. 88 Responden 7 (Lanjutan)

		4	Apakahpersonel yang dapat masuk ke secure area sudah sesuai dengan kebijakan organisasi?	✓	
		5	Apakah kontrol entri terhadap secure area *direview* apabila ditemukan perubahan terhadap suatu kondisi?	✓	
A.11.1.3	Mengamankan kantor, kamar, dan fasilitas	1	Apakah ruangan kantor dan fasilitas lain telah dirancang dan dikonfigurasi dengan mempertimbangkan keamanan?	✓	
		2	Apakah terdapat proses untuk menjaga keamanan (misalnya mengunci, membersihkan meja, dll.)?	✓	

		3	Apak terkait keamanan ruangan sudah dikomunikasikan dengan baik kepada karayawan?		✓
		4	apakah ruangan kantor sudah sesuai dengan suatu standar?		✓
		5	Apakah dilakuna *review* terhadap keamanan kantor atau ruangan apabila ditemukan perubahan suatu kondisi?	✓	
A.11.1.4	Melindungi dari ancaman eksternal dan lingkungan	1	Apakah perlindungan fisik untuk mencegah bencana alam, serangan jahat atau kecelakaan telah dirancang?		✓
		2	Apakah perlindungan fisik terkait ancaman bencana alam atau serangan jahat sudah disetujui oleh manajemen?		✓
		3	Apakah perlindungan fisik sudah terdukomentasi?		✓
		4	Apakah perlindungan fisik terkait ancaman bencana alam dan pihak jahat sudah sesuai standar keamanan?		✓
		5	Apakah dilakukan *review* terkait rancanagan perlindungan fisik apabila ditemukan perubahan suatu kondisi?	✓	
A.11.1.5	Bekerja di tempat yang aman	1	Apakah terdapat area aman *(Secure Area)?*	✓	
		2	Apakah s*ecure area* memiliki kebijakan dan proses yang sesuai?		✓
		3	Apakah kebijakan dan proses dilakukan dan dipantau?		✓
		4	Apakah secure area sudah distujui organisasi?	✓	
		5	Apakah dilakukan *review* terkait secure area apabila ditemukan perubahan pada suatu kondisi?	✓	
A.11.1.6	Area pengiriman dan pemuatan	1	Apakah terdapat area pengiriman / pemuatan yang terpisah?	✓	

Tabel lampiran D. 89 Responden 7 (Lanjutan)

		2	Apakah akses ke area pengiriman/pemuatan dikendalikan?		✓
		3	Apakah akses area pemuatan diisolasi dari fasilitas pemrosesan informasi?	✓	
		4	Apakah secure area sudah distujui organisasi?		✓
		5	Apakah dilakukan *review* terkait secure area apabila ditemukan perubahan pada suatu kondisi?	✓	
A.11.2	Peralatan		Pertanyaan	Ya	Tidak

A.11.2.1	Penempatan dan perlindungan peralatan	1	Apakah bahaya lingkungan diidentifikasi dan dipertimbangkan ketika lokasi peralatan dipilih?	✓	
		2	Apakah risiko akses yang tidak sah telah dipertimbangkan saat menentukan lokasi peralatan?		✓
		3	Apakah penempatan peralatan sudah terdokumentasi?	✓	
		4	Apakah penempatan peralatan sudah seuasuai dengan kebutuhan organisasi?		✓
		5	Apaha dilakukan *review* terkait penempatan dan perlindungan peralatan apabila ditemukan perubahan suatu kondisi?	✓	
A.11.2.2	Utilitas pendukung	1	Apakah terdapat UPS atau generator cadangan?	✓	
		2	Apakah sistem UPS sudah diuji dalam skala waktu yang sesuai?		✓
		3	Apakah UPS yangdigunakan sudah berdasarkan suatu standar?	✓	
		4	Apakah penggunaan UPS sudah berdasarkan kebutuhan organisasi?	✓	
		5	Apakah terdapat mekanisme *review* terkait penggunaan UPS apabila ditemukan perubahan suatu kondisi?	✓	
A.11.2.3	Keamanan kabel	1	Apakah penilaian risiko telah dilakukan atas lokasi kabel listrik dan kabel telekomunikasi atau jaringan?	✓	
		2	Apakah kabel listrik dan jaringan ditempatkan supaya terlindung dari gangguan, intersepsi, atau kerusakan?	✓	
		3	Apakah penempatan kabel lstrik dan jaringan sudah terdokumentasi?		✓

Tabel lampiran D. 90 Responden 7 (Lanjutan)

		4	Apakah penentuan tempat kabel listrik dan jaringan sudah berdasarkan penilaian ancaman bencana alam dan ancaman pihak jahat?	✓	
		5	Apakah dilakukan *review* terkait penempatan posisi kabel dan ajaringan apabila ditemukan perubahan suatu kondisi?	✓	
A.11.2.4	Perawatan peralatan	1	Apakah terdapat jadwal perawatan peralatan yang ketat?	✓	
		2	Apaakah perawatan peralatan diketahui oleh manajemen?	✓	
		3	Apakah perawatan peralatan terdokumentasi?		✓

		4	Apakah perawatan peralatan keamanan sudah sesuai dengan standar kemanan?		✓□
		5	Apakah dilakukan *review* terkait terawatan keamanan apabila ditemukan perubahan suatu kondisi?	✓□	
A.11.2.5	Penghapusan perangkat	1	Apakah terdapat proses yang mengontrol bagaimana perangkat dihapus dari daftar perangkat?	✓□	
		2	Apakah proses kontol penghapusan perangkat dilakukan?		✓□
		3	Apakah pemeriksaan langsung terhadap proses penghapusan perangkat dilakukan?		✓□
		4	Apakah pengahapusan perangkat sudah disetujui oleh manajemen dan pimpinan?		✓□
		5	Apakah dilakukan *review* terkait penghapusan perangkat dari daftar peranghat apabila ditemukan perubahan suatu kondisi?	✓□	
A.11.2.6	Keamanan peralatan dan perangkat di luar lokasi	1	Apakah terdapat kebijakan yang mengatur keamanan perangkat di luar lokasi?	✓□	
		2	Apakah kebijakan perlindungan perangkat diluar lokasi (kantor) dikomunikasikan secara luas?		✓□
		3	Apakah penempatan perlatan diluar lokasi terdokumentasi?		✓□
		4	Apakah penempatan perlatan diluar lokasi sudah memperhitungkan bahaya keamanan bencana alam atau ancaman prilaku jahat?	✓□	
		5	Apakah dilakukan *review* terkait perlindungan peralatan diluar lokasi?	✓□	

Tabel lampiran D. 91 Responden 7 (Lanjutan)

A.11.2.7	Pembuangan yang aman atau penggunaan kembali peralatan	1	Apakah terdapat kebijakan yang mengatur bagaimana perangkat informasi dapat digunakan kembali?	✓□	
		2	Apakah mekanisme pengelolaan data, diverifikasi dengan benar sebelum digunakan kembali / dibuang?	✓□	
		3	Apakah kebijakan penggunaan atau pembuanagan data sudah dikomunikasikan secara baik kepada karyawan?		✓□

		4	Apakah pembuangan atau penggunaan kembali peralatan sudah berdasarkan pertimbangan keamanan?		✓□
		5	Apakah terdapat mekanisme *review* terkait penggunaan atau pembuangan apabila ditemukan perubahan suatu kondisi?	✓□	
A.11.2.8	Peralatan pengguna tanpa pengawasan	1	Apakah organisasi memiliki kebijakan tentang bagaimana peralatan yang tidak dijaga harus dilindungi?		✓□
		2	Apakah kontrol teknis diterapkan untuk mengamankan peralatan yang secara tidak sengaja ditinggalkan?		✓□
		3	Apakah terdapat pendokumentasian terhadap barang - barang yang tidak sengaja ditinggalkan?		✓□
		4	Apakah kebijakan terkait perlindungan perlatan yang tidak sengaja ditinggalkan sudah diketahui pimpinan dan manajemen?		✓□
		5	Apakah dilakukan *review* terkait kebijakan perlindungan barang yang tdaik sengaja ditinggalkan?	✓□	
A.11.2.9	Kebijakan *Clear desk and clear screen*	1	Apakah terdapat kebijakan *clear desk /clear screen?*	✓□	
		2	Apakah kebijakan clear desk dan clear screen diberlakukan dengan baik?	✓□	
		3	Apakah kebijakan terkait clear screen dan clear desk sudah dikomunikasikan dengan baik dengan karyawan?	✓□	
		4	Apakah kebijakan clear screen dan clear desk sudah sesuai dengan kebutuhan organisasi?		✓□
		5	Apakah dilakukan *review* terhadap kebijakan clear screen dan clear desk apabila ditemukan perubahan suatu kondisi?	✓□	

LAMPIRAN E

PEMBOBOTAN

Tabel Lampiran E. 1 Pembobotan Domain A.5

Domain A.5 : Kebijakan keamanan informasi																
Domain A.5.1 : Arahan manajemen untuk keamanan informasi																
Domain A.5.1.1 : Kebijakan untuk keamanan informasi																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Terdapat kebijakan keamanan informasi terkait pengolahan informasi	Kebijakan informasi sudah ada, namun masih bersifat lisan disampaikan kepada karyawan UPTTIK oleh ketua.	0	2	4	1	0	0	7	0	2	8	3	0	0	13	1,85

Domain A.5.1.2 : Review kebijakan untuk keamaan informasi											
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden	Jumlah	Jumlah / Responden

Review terhadap kebijakan untuk keamanan informasi	Review kebijakan untuk kemanan informasi tidak dilakukan secara berkala, namun hanya dilakukan apabila terjadi atau ditemukan perubahan situasi terkait keamanan informasi	1	4	2	0	0	0	7	0	4	4	0	0	0	8	1,14

Tabel Lampiran E. 2 Pembobotan Domain A.6

Domain A.6 : Keamanan informasi organisasi																
Domain A.6.1 : Internal organisasi																
Domain A.6.1.1 : Peran dan tanggungjawab keamanan informasi																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Peran dan tanggungjawab terhadap keamanan informasi organisasi	Peran dan tanggungjawab terhadap keamanan informasi sudah dilakukan oleh organisasi, namun hanya bersifat lisan dan belum memiliki dokumen panduan, dari penelitian juga diketahui bahwa tidak semua karyawan faham terkait peran dan perlindungan keamanan informasi organisasi.	0	1	4	2	0	0	7	0	1	8	6	0	0	15	2,14

Domain A.6.1.2 : Pemisahan tugas																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Terdapat mekanisme pemisahan tugas dalam pengelolaan tugas berdasarkan keahlian masing-masing	Mekanisme pemisahan tugas sudah dilakukan secara tertulis dan terdokumentasi, masing - masing karyawan ditempatkan pada bagian masing - amasing berdasarkan keahlian masing - masing.	0	2	3	2	0	0	7	0	2	6	6	0	0	14	2

Domain A.6.1.3 : Kontak dengan pihak berwenang																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Terdapat mekanisme yang mengatur tentang kontak dengan pihak berwenang, misalnya terkait dengan kejadian serangan keamanan.	Terkait dengan terjadinya suatu insiden terdapat mekanisme atau alur dalam penanggulangan masalah, contohnya terjadi masalah pada server aplikasi SIMAK yang menyebabkan berhentinya aplikasi, namun mekanisme dilakukan secara kebiasaan dan belum mengikuti suatu panduan dan belum terdokumentasi.	1	4	1	1	0	0	7	0	4	2	3	0	0	9	1,28

Domain A.6.1.4 : Kontak dengan kelompok minat khusus																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Terdapat mekanisme terkait kontak dengan group khusus, misalnya dengan group atau forum keamanan saiber.	Masing - masing karyawan mempunyai tugas dan fungsi yang berbeda, termasuk dalam hal kontak dengan grup atau komunitas khusus terkait dengan keamanan informasi, misalnya karyawan bagian developer SIMAK ditugaskan oleh pimpinan dalam meningkatkan pengetahuan dalam hal pengembangan aplikasi.	2	3	2	0	0	0	7	0	3	4	0	0	0	7	1

Domain A.6.1.5 : Keamanan informasi dalam manajemen proyek																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Terdapat penilaian keamanan terkait seluruh proyek , penilaian proyek dilakukan secara rutin pada setiap tahapan.	Penilaian terkait keamanan dalam proyek dilakukan, namun tidak rutin, penilaian hanya dilakukan apabila ditemukan suatu kejadian terkait keamanan, selain itu juga belum terdokumentasi dengan baik. Penilaian keamanan belum mengacu pada suatu panduan secara resmi, hanya berdasarkan pengalaman dari karyawan yang menilai.	1	2	4	0	0	0	7	0	2	8	0	0	0	10	1,42

Domain A.6.2 : Perangkat seluler dan kerja jarak jauh *(Teleworking)*																
Domain A.6.2.1 : Kebijakan terkait perangkat seluler																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Terdapat kebijakan perangkat seluler yang terkait dengan keamanan informasi	Kebijakan terkait perangkat selular hanya berupa himbauan keamanan, berupa banner yang berisi saran agar berhati - hati dalam pengaksesan jaringan dan installasi program. Banner himbauan disebarkan ke seluruh fakultas yang ada di Universitas Siliwangi.	1	3	2	1	0	0	7	0	3	4	3	0	0	10	1,42

Domain A.6.2.2 : Kerja jarak jauh *(Teleworking)*																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Terdapat kebijakan mengenai kerja jarak jauh atau Teleworking	Tedapat kebijakan bagi karyawan yang an melakukan *teleworking* atau kerja jarak jauh, manajemen tidak memberikan arahan secara lengkap terkait dengan keamanan lingkungan yang dijadikan *teleworking*, jaringan yang dipakai untuk mengakases server aplikasi SIMAK. karyawan yang melakukan teleworking juga tidak melakukan dokumentasi tentang hasil kerjanya.	0	3	4	0	0	0	7	0	3	8	0	0	0	11	1,57

Tabel Lampiran E. 3 Pembobotan Domain A.9

Domain A.9 : Kontrol akses																
Domain A.9.1 : Persyaratan bisnis terkait kontrol akses																
Domain A.9.1.1 : Kebijakan kontrol akses																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Terdapat kebijakan terkait kontrol akses bagi pengguna	Kebiajakn terkait kontrol akses terhadap aplikasi SIMAK diatur berdasarkan kebijakan yang dikeluarkan oleh pimpinan UPTTIK, kebijakan belum tertulis, dan masih berupa arahan secara lisan dari pimpinan, kebijakan belum mengacu pada suatu standar, kebijakan dikeluarkan berdasarkan kebiasaan yang diwariskan dari kepemimpinan terdahulu.	0	3	4	0	0	0	7	0	3	8	0	0	0	11	1,57

Domain A.9.1.2 : Akses ke jaringan dan layanan jaringan																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Terdapat kontrol untuk memastikan pengguna hanya memiliki kontrol ke jaringan berdasarkan haknya.	Karyawan yang bertugas sebagai programmer menggunakan jaringan privat dalam mengakases server aplikasi SIMAK, hal ini diatur oleh kebijakan yang keluarkan oleh pimpinan UPTTIK, namun begitu kebijakan dan akses belum terdokumentasi dengan baik. Sedangkan bagi karyawan yang hanya berhak mengakses aplikasi SIMAK dengan level biasa bisa menggunakan jaringan yang digunakan pengguna seca umum.	1	4	2	0	0	0	7	0	4	4	0	0	0	8	1,14

Domain A.9.2 : Manajemen akses pengguna																
Domain A.9.2.1 : Pendaftaran dan pencabutan hak akses pengguna																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Proses pendaftaran dan pencabutan akases pengguna terhadap layanan atau sistem informasi	Proses pendafran dan bencabuatan hak akses bagi pengguna sudah dilakukan, pengguna yang berpindah unit kerja di cabut hak aksesnya terhadap aplikasi SIMAK (pemrosesan data) dan hanya dapat mengakses aplikasi sesuai dengan unit kerja barunya, juga terhadap server, dicabut atau diahapus, pendaftaran, pencabutan atau pembatalan hak akses dilakukan oelh superadmin berdasarkan arahan dari kepala UPTTIK. Namun begitu tahapan atau langkah ini belum terdokumentasi dengan baik.	0	2	3	1		1	7	0	2	6	3	0	0	11	1,57

Domain A.9.2.2 : Penyediaan akses pengguna																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Terdapat proses penyediaan akses bagi pengguna dan penetapan hak akses pada layanan	Penyediaan akases pengguna dilakukan oleh pemegang sistem, seperti pengguna (karyawan) baru di daftarkan terhadap sistem atau aplikasi SIMAK, pemegang sistem mem-verifikasi tingkat atau hak akses karayawan baru tersebut, level akses di cocokan dengan tugas dan fungsi karyawan sesuai dengan surat keputusan yang ia miliki sebagai pegawai. Proses ini dilakukan secara formal oleh pemilik akses utama.	0	1	3	3	0	0	7	0	1	6	9	0	0	16	2,28

Domain A.9.2.3 : Pengelolaan hak akses istimewa																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Terdapat mekanisme terkait pengelola hak akses istimewa (admin dan super admin) pada sistem.	Pengeloaan super admin dilakukan berdasarkan tugas dan fungsi karayawan, tidak semua karyawan UPTTIK mempunyai hak akses sebagai super admin pada aplikasi maupun server aplikasi SIMAK, penentuan akses sebagai super admin dapat dilakukan juga terkait kebutuhan tertentu, misalnya bagian akademik memerlukan akses terkait pengelolaan suatu data, maka akses dapat dibuat berdasarkan surat keterangan.	0	3	3	0	0	1	7	0	3	6	0	0	5	14	2

Domain A.9.2.4 : Pengelolaan informasi rahasia																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Terdapat proses atau manajemen pengelolaan informasi rahasia secara formal.	Pengelolaan informasi rahasia sudah dilakukan, karyawan di UPTTIK harus menjaga data sensitif dan juga dilarang membagikan data yang bersifat sensitif atau arahasia kepada piahak luar, namun meski begitu, belum ada dokumentasi dan peraturan secara tertulis terkait kebijakan tersebut.	2	3	2	0	0	0	7	0	3	4	0	0	0	7	1

Domain A.9.2.5 : Review hak akses pengguna																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Pemilik aset meninjau hak akses pengguna secara berkala terkait perubahan suatu kondisi seperti kenaikan pangkat dan lain sebagainya.	Terkait hak akses pengguna, tidak ada mekanisme yang mengatur bahwa UPTTIK sebagai pemegang sistem atau aplikasi SIMAK harus meninjau atau me-review hak aksesnya, namun peninjauan dilakukan berdasarkan ajuan dari pengguna. Proses peninjauan dilakukan secara tidak rutin dan belum ada dokumentasi terkait hal itu.	3	1	3	0	0	0	7	0	1	3	0	0	0	4	0,57

Domain A.9.2.6 : Penghapusan atau penyesuaian hak akses pengguna																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Hak akses pengguna terhadap sistem dan atau pemrosesan sistem harus dihapus ketika pemutusan hubungan kerja.	Ketika seorang karyawan tidak lagi bekerja pada suatu bagian, maka akses terhadap aplikasi SIMAK juga di cabut, begitu juga ketika pengguna pindah ke bagian lain, maka hak akses terhadap aplikasi SIMAK di sesuaikan sesuai dengan ketentuan yang baru.	1	2	4	0	0	0	7	0	2	8	0	0	0	10	1,42

Domain A.9.3 : Tanggungjawab																
Domain A.9.3.1 : Penggunaan informasi rahasia																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Terdapat dokumen tentang panduan pengelolaan data atau informasi rahasia.	Terkait pengelolaan data rahasia pada aplikasi SIMAK, UPTTIKK belum mempunyai dokumen yang mengatur hal itu, namun segala bentuk pengelolaan data sensitif atau rahasia tetap dilakukan, namun hanya berdasarkan arahan kepala UPTTIK, proses pengelolaan dilakukan belum terdokumentasi.	2	4	1	0	0	0	7	0	4	1	0	0	0	5	0,71

Domain A.9.4. : Kontrol akses sistem dan aplikasi																
Domain A.9.4.1 : Pembatasan akses informasi																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Akses terhadap sistem atau aplikasi telah dibatasi sesuai kebijakan organisasi.	Akses terhadap aplikasi SIMAK dibatasi sesuai dengan kebutuhan dan kebijakan organisasi, kebijakan tersebut berupa kebijakan lisan yang diterjemahkan dari peraturan atau kebijakan pimpinan. Pembatasan akses dilakukan oleh pemegang sistem, pembatasan belum terdokumentasi.	0	2	5	0	0	0	7	0	2	10	0	0	0	12	1,71

Domain A.9.4.2 : Prosedur log-on																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Terdapat prosedur log-on yang aman untuk mengamankan aplikasi agar terhindar dari akses yang tidak sah.	Aplikasi SIMAK diamankan oleh prosedur *log-on*, dimana prosedur *log-on* ini mengharuskan pengguna untuk login terhadap aplikkasi SIMAK untuk dapat mengakses data atau mengolah data didalamnya. Prosedur ini dilakukan untuk emngamankan data dari akses yang tidak sah.	0	2	4	1	0	0	7	0	2	8	3	0	0	13	1,85

Domain A.9.4.3 : Sistem manajemen kata sandi *(password)*																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Aplikasi diamankan oleh manajemen kata sandi, kata sandi yang dipakai haruslah berkualitas.	Manajemen pengolahan kata sandi aplikasi SIMAK masih menerima *password* dengan karakter sederhana, sistem belum dirancang untuk mengharuskan pengguna menggunakan atu menginputkan kata sandi yang rumit misalnya kombinasi antara huruf, angka dan simbol, hal ini bisa jadi kelemahan yang dapat berisiko terhdapat keamanan data.	0	4	2	1	0	0	7	0	4	4	3	0	0	11	1,57

Domain A.9.4.4 : Penggunaan program utilitas dengan hak istimewa																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Terdapat pemantauan terkait program utilitas yang dapat digunakan oleh pengguna.	Program utilitas pada aplikasi SIMAK seperti fitur untuk menghapus, mengimport dan mengeksport data masih belum diawasi, beberapa kasus pernah terjadi terkait menu utilitas, seperti terhapusnya data, ini tentu saja sangat berbahaya, karena integritas data dapat terancam oleh kases yang tidak sah. Pendokumentasian, pembatasan dan pematauan mutlak dilakukan untuk memantau program utilitas pada aplikasi SIMAK.	0	4	2	1	0	0	0	0	4	4	3	0	0	11	1,57

Doamain A.9.4.5 : Kontrol akses terhadap *source code*																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Source code dipisahkan dan diamankan oleh kontrol akses, hanya pengguna dengan hak akses tertentu yang dapat mengakses *source code* atau kode sumber dsari sistem atau aplikasi.	Kode sumber atau *source code* aplikasi SIMAK diamankan oleh hak akses, hanya orang yang mempunyai akses tertentu saja yang dapat mengakses kode sumber tersebut, pengguna harus menggunakan VPN untuk dapat mengakses kode sumber tersebut, namun belum ada kebijakan atau peraturan yng mengatur terkait siapa saja yang dapat mengakses kode sumber tersebut.	0	1	4	2	0	0	7	0	1	8	6	0	0	15	2,14

Tabel Lampiran E. 4 Pembobotan Domain A.11

Domain A.11.1.2 : Kontrol entri fisik																	
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Secure area memiliki sistem pengamanan secara fisik, sehingga hanya orang yang berwenang saja yang dapat masuk kedalam *secure area.*	*Secure area* atau area aman terdapat pada UPTTIK, yang pertama adalah bagian luar, tengah dan dalam, pada ruangan dalam (ruang server) juga sudah di rancang sebagai ruangan aman untuk bekerja, petugas yang bertugas memelihara server aplikasi SIMAK dapat bekerja secara aman, baik dari gangguan bencana alam ataupun dari gangguan lain seperti aliran listrik dan lain sebagainya.	0	2	3	1	0	1	7	0	2	6	3	0	5	16	2,28

Domain A.11.1.3 : Mengamankan ruangan kator dan fasilitas lainnya.																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Ruangan kantor dan ruangan server dalam perancangannya telah mempertimbangkan dan di konfogurasi agar terhindar dari gangguan keamanan	Ruangan kantor dan ruangan server aplikasi UPTTIK pada perancangannya tidak mengacu pada rancangan bangunan yang di peruntukan untuk server, namun meski begitu keamanan standar seperti dinding pembatas, dinding beton dan kunci keamanan telah terpasang untuk mengamankan ruangan UPTTIK dan ruangan server dari gangguan,baik gangguan alam maupun gangguan akses jahat.	0	2	4	1	0	0	7	0	2	8	3	0	0	13	1,85

Domain A.11.1.4 : Terlindungi dari ancaman eksternal dan lingkungan																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Ruangan server telah dirancang agar terlindung dari ancaman eksternal dan lingkungan seperti bencana alam dan perbuatan jahat.	Ruangan server aplikasi SIMAK tidak dirancang sebagai ruangan server, ada beberapa kelemahan yang dapat menjadi ancaman bagi keamanan data atau pengguna, seperti kabel jaringan dan kabel listrik tidak dipisahkan jalurnya, tidak ada pendingan yang khusus di peruntukan untuk ruangan server, jalur kabel tidak melalui jalur nawah lantai, dan beberapa kelemahan lainnya, kelemahan kelemhan tersebut dapat menjadi ancaman, baik ancaman alam ataupun ancamn yang berasal dari gangguan manusia.	1	4	2	0	0	0	7	0	4	4	0	0	0	8	1,14

Domain A.11.1.5 : Bekerja pada area yang aman *(secure area)*																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Terdapat *secure area* atau area aman untuk bekerja, area aman diartikan aman dari gangguan internal dan eksternal, pada area ini foto dan vidio dilarang digunakan tanpa seizin atau ketentuan organisasi	Terdapat area aman untuk bekerja pada UPTTIK, selruh ruangan pada UPTTIK disesuaikan agardapat menjadi ruangan yang aman untuk bekerja, juga ruangan server aplkasi SIMAK telah disesuaikan untuk menjadi secure area, namun meski begitu *secure area* belum berdasarkan suatu standar keamanan tertentu.	0	2	3	2	0	0	7	0	2	6	6	0	0	8	1,14

Domain A.11.1.6 : Area pengiriman dan pemuatan																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Terdapat area pengiriman dan pemuatan yang terpisah, area ini dikendalikan oleh bagian yang berwenang.	Area pengiriman dan pemuatan barang dikelola dan dikendalikan oleh bagian khusus, namun bukan oleh karyawan dari UPTTIK, seluruh barang yang di tujukan eke UPTTIK diperiksa dan dicatat oleh bagian yang bertugas mengelola barang. Mekanisme pemeriksaan barang tidak berdasarkan pada standar keamanan, dan hanya berupa pengecekan biasa terhadap kesesuaian barang.	0	2	3	0	0	2	7	0	2	6	0	0	10	18	2,57

Domain A.11.2 : Peralatan																
Domain A.11.2.1 : Penempatan dan perlindungan peralatan																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Bahaya diidentifikasi saat penentuan penempatan bagi peralatan yang akan dipasang, risiko akses tidak sah di pertimbangkan ketika menetukan lokasi alat.	Terdapat pengidentifikasian lokasi tempat barang akan di tempatkan, pemilihan lokasi berdasarkan peniliaian keamanan dan ancaman, ancaman berupa ancaman internal maupun ancaman eksternal. Contohnya kertika pemilihan lokasi jalur kabel jaringan, pemilihan lokasi rack UPS telah mempertimbangkan potensi ancamn yang akan muncul, baik ancaman manusia ataupun alam.	0	1	3	3	0	0	7	0	1	6	9	0	0	16	2,28

Domain A.11.2.2 : Utilitas pendukung																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Terdapat *backup* energi cadangan berupa UPS, UPS sudah diuji dan berfungsi normal, dapat mem-*backup* energi untuk server selama kurang lebih dua jam.	Server aplikasi SIMAK telah menggunakan UPS sebagai daya cadangan ketika aliran listrik mati, UPS dapat mem-*backup* daya selama kurang lebih 2 jam, namun hal itu bukan berdasarkan suatu panduan keamanan.	0	1	2	3	0	1	7	0	1	4	9	0	5	19	2,71

Domain A.11.2.3 : Keamanan kabel																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Penilaian risiko telah di perhatikan ketika penempatan kabel listrik dan jaringan, sehingga dapat terhindar dari gangguan, baik gangguan alam atau gangguan dari akses yang tidak sah.	Penilaian keamanan kabel jaringan dan kabel listrik telah dilakukan ketika memilih lokasi penempatannya, pemilihan lokasi bertujuan agar kabel lsitrikk dan jaringan jauh atau terhindar dari gangguan, namun meski demikian pemilihan lokasi hanya berdasarkan asumsi, buka merujuk pada satu panduan keamanan.	0	2	4	1	0	0	7	0	2	8	3	0	0	13	1,85

Domain A.11.2.4 : Perawatan peralatan																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Terdapat jadwal perawatan peralatan yang ketat terhadap alat - alat server dan alat - alat pendukung lainnya.	Perawatan terhadap alat - alat server kerap kali dilakukan, tidak ada jadwal rutin yang mengharuskan atau mengatur kapan peralatan server aplikasi SIMAK harus dirawat, perawatan dilakun apabila ditemukan perubahan suatu kondisi yang menyebabkan terganggunaya kinerja sever..	1	1	2	3	0	0	7	0	1	4	9	0	0	14	2

Doamain A.11.2.5 : Penghapusan perangkat																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Terdapat proses yang mengatur tentang penghapusan perangkat, kontrol proses penghapusan dikendalikan oleh bagian yang berwenang.	Proses penghapusan perangkat dilakukan oleh bagian yang bertugas mengelola barang, UPTTIK sebagai pemakai hanya memastikan bahawa barang yang masukan ke dalam daftar aset yang akan dihapus benar - benar sudah tidak dapat digunakan kembali dan memastikan tidak ada lagi data sensitif pada barang yang akan di hapus.	0	3	3	1	0	0	7	0	3	6	3	0	0	12	1,71

Domain A.11.2.6 : Keamanan peralatan dan perangkat di luar lokasi																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Terdapat kebijakan terkait pengendalian peralatan yang berada di luar lokasi, barang harus dipastikan terjamin keamanannya, seperti risiko pencurian, penayadapan dan risiko keamanan lain yang dapat menagancam keamanan perangakat yang erada di luar lokasi oraganisasi.	Kebiajakan terkait keamanan perangkat yang ditempatkan diluar lokasi telah ada, namu hanya berupa intrukksi dari pimpinan UPTTIK secara lisan dan belum terdokumentasi.	0	2	4	1	0	0	7	0	2	8	3	0	0	13	1,85

Domain A.11.2.7 : Pembuangan yang aman atau penggunaan kembali																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Terdapat kebijakan dan mekanisme yang menagatur terkait pembuangan atau penggunaan kembali alat, seperti pada hardisk atau media penyimpanan lainnya harus dipastiakan tidak mengandung data - data yang sensitif, atau abahkan *software* yang berlisensi.	Barang yang akan di buang atau di gunakan lagi diperiksa oleh masing - masing penanggungjawab atas barang tersebut, pemegang barang harus benar-benar memastikan barang yang dikelolanya ketika akan di buang atau tidak di gunnakan lagi benar - benar kosong atau tidak mengandung data sensitif, juga barang yang akan di b uang tidak lagi memiliki lisensi software didalamnya.	0	1	4	2	0	0	7	0	1	8	6	0	0	15	2,14

Domain A.11.2.8 : Peralatan pengguna tanapa pengawasan																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Organisasi memilki kebijakan terkait bagaimana peralatan yang dia pakai harus diamankan, seperti emenghentikan sesi aktif ketika tidak digunakan, keluar atau *log-out* aplikasi dan lainnya.	Kebijakan terkait perlindungan peralatan yang dipakai oleh karyawan di komunikasikan secara lisan oleh pimpinan kepada seluruh karyawan, pimpinan memberikan arahan terhadap pengguna untuk mengamankan perangkat yang ia gunakan, pengkentikan sesi aktif, mel-*logout* aplikasi, hal ini bertuja supaya tidak ada ases ilegal oleh orag yag tidak bertaggugjawab terhadap aplikasi SIMAK.	2	3	2	0	0	0	7	0	3	4	0	0	0	7	1

Domain A.11.2.9 : Kebijakan untuk *clear-desk* dan *clear-screen*																
Pernyataan	Hasil Pemeriksaan	0	1	2	3	4	5	Responden	Banyak * Responden						Jumlah	Jumlah / Responden
Terdapat kebijakan *clear-desk* dan *clear-screen,* catatan yan mengandung data sensitif harus bersih dari meja atau komputer, komputer juga harus terlundung dengan cara mengguanakan PIN dan lain sebagainya.	Pimpian menhimbau kepada seluruh karyawan untu kerbiasa dengan kebijakan *clear desk* dan *clear screen* , hal ini dimaksudkan supaya tidak ada data data sensitif yang tertinggal pada meja yang bisa saja dimanfaatkan oleh orang yang tidak bertanggungjawab, data dapat berupa catatan *password* dan kode akses lainnya, misalkan kode akses untuk mengakses server aplikasi SIMAK.	0	3	3	1	0	0	7	0	3	6	3	0	0	12	1,71