LAPORAN
ANALISIS KINERJA TATA KELOLA TI

UIN
RADEN FATAH
PALEMBANG

MENGGUNAKAN ISO/IEC 27002:2013 PADA UIN RADEN FATAH PALEMBANG

LAPORAN ANALISIS KINERJA TATA KELOLA TI MENGGUNAKAN ISO/IEC 27002:2013 PADA UIN RADEN FATAH PALEMBANG

PUSAT TEKNOLOGI INFORMASI DAN PANGKALAN DATA

UNIVERSITAS ISLAM NEGERI RADEN FATAH

PALEMBANG

2022

EXECUTIVE SUMMARY

Berdasarkan tinjauan dan analisis kinerja tata kelola TI yang telah dilakukan di UIN Raden Fatah Palembang, disimpulkan bahwa proses keamanan sistem informasi yang berjalan saat ini belum sesuai dengan standar ISO/IEC 27002:2013. Hal ini dikarenakan dari total 14 implementasi klausul ISO/IEC 27002:2013 pada UIN Raden Fatah, masih ditemukan beberapa implementasi yang belum sesuai maupun belum dilakukan berdasarkan standar keamanan ISO/IEC 27002:2013. Sehingga menghasilkan rekomendasi untuk beberapa kontrol keamanan yang memerlukan perbaikan, sebagai bahan evaluasi untuk organisasi memperbaiki tata kelolaTI yang belum berjalan optimal sesuai dengan standar manajemen keamanan informasi.

Selain itu diperoleh hasil tingkat kemampuan *(capability level)* dan tingkat kematangan *(maturity level)* untuk keamanan sistem informasi UIN Raden Fatah, yaitu sama-sama terletak pada level 2 *(managed)* dengan nilai *capability level* sebesar 1,96 dan *matury level* sebesar 2,34. Hal ini menunjukkan bahwa baik proses tingkat kemampuan maupun tingkat kematangan dalam mengelola keamanan sistem informasi pada UIN Raden Fatah saat ini sudah menerapkan pengelolaan proses keamanan sistem informasi yang mengikuti prosedur yang berstandar dari organisasi sendiri, namun masih bersifat umum dan belum mengacu atau berpedoman pada standar manajemen keamanan informasi secara khusus.

Maka agar proses keamanan sistem informasi pada UIN Raden Fatah berlangsung dengan proses yang baik dan tepat sesuai dengan manajemen keamanan informasi, maka diperlukan terlebih dahulu perbaikan pada C.5

Kebijakan keamanan sistem informasi. Hal ini dikarenakan klausul ini merupakan implementasi klausul pertama yang harus terlebih dahulu diperbaiki dengan memiliki dan melengkapi serangkaian dokumen kebijakan keamanan sistem informasi yang ada pada UIN Raden Fatah sesuai dengan rekomendasi C.5 pada ISO/IEC 27002:2013.

Diharapkan dokumen kebijakan yang sudah dibuat tersebut dapat menjadi petunjuk implementasi untuk klausul-klausul lainnya dalam mengimplementasi proses keamanan sistem informasi pada UIN Raden Fatah sesuai dengan standar manajemen keamanan informasi. Sehingga hal ini akan berdampak baik untuk meningkatkan tingkat kemampuan *(capability level)* dan tingkat kematangan *(maturity level)* keamanan pada UIN Raden Fatah, karena proses yang berjalan nantinya sudah tidak lagi bersifat umum tetapi sudah mengadopsi standar manajemen keamanan informasi.

DAFTAR ISI

Halaman

KATA PENGANTAR

Puji syukur dengan menyebut nama Allah SWT yang telah mencurahkan rahmat, taufik, dan hidayah-Nya, sehingga laporan Evaluasi Tata Kelola Keamanan Sistem Informasi Menggunakan ISO/IEC 27002:2013 pada UIN Raden Fatah Palembang dengan baik. Evaluasi Tata Kelola Keamanan Sistem Informasi ini dilakukan sebagai upaya untuk memeriksa dan memperbaiki tata kelola keamanan sistem informasi pada UIN Raden Fatah yang belum secara optimal berjalan sesuai sistem standar manajemen keamanan informasi. Diharapkan dengan adanya laporan evaluasi ini, dapat menjadi bahan pertimbangan dan evaluasi untuk perbaikan terhadap tata kelola keamanan sistem informasi yang belum sesuai, sehingga tata kelola keamanan sistem informasi pada UIN Raden Fatah dapat terus berkembang dan bekerja secara optimal.

Palembang, Oktober 2022

Rusmala Santi, M.Kom

NIP. 197911252014032002

BAB I
PENDAHULUAN

1.1 Latar Belakang

Universitas Islam Negeri (UIN) Raden Fatah merupakan lembaga perguruan tinggi di Sumatera Selatan yang berbasis Islami. Karena merupakan lembaga besar yang menyangkut banyak orang, terkait dengan aset data informasi dan penggunaan sistem informasi sebagai media pembantu pekerjaan saat ini, maka UIN Raden Fatah perlu melakukan evaluasi tata kelola keamanan sistem informasi untuk memeriksa apakah tata kelola keamanan sistem informasi pada UIN Raden Fatah sudah memiliki keamaan berstandar sistem manajemen keamanan informasi yang berlaku atau tidak.

Evaluasi tata kelola keamanan sistem informasi merupakan hal yang perlu dan penting untuk diimplementasikan pada sebuah organisasi, karena dengan perkembangan teknologi yang semakin canggih, dapat mengancam kerahasiaan data dan integritas data organisasi. Maka dari itu evaluasi tata kelola keamanan sistem informasi dapat membantu organisasi untuk meningkatkan tingkat keamanan informasi yang dimilikinya, karena evaluasi tata kelola merupakan kegiatan yang bersifat kontinu, sehingga organisasi dapat melihat dan mengevaluasi kinerja tata kelola sistem keamanan sistem informasi yang dimilikinya, apakah sudah sesuai dan mengalami peningkatan atau sebaliknya.

Saat organisasi memutuskan untuk melakukan evaluasi, maka diperlukan sebuah standar ataupun *framework* sebagai pedoman bagi evaluator, agar hasil evaluasi dapat dinyatakan legal sehingga dapat dipertanggungjawabkan. Dengan menggunakan ISO/IEC 27002:2013 sebagai standar evaluasi tata kelola keamanan sistem informasi, yang berisikan pedoman kode praktik sistem manajemen keamanan informasi. Standar ini memberikan kontrol keamanan informasi yang disertai dengan panduan implementasi bagi evaluator dalam memperbaiki temuan yang memerlukan perbaikan, sehingga dapat membantu penyelesaian masalah yang mengancam keamanan sistem informasi pada suatu organisasi. Standar ISO/IEC 27002:2013 ini tidak hanya membahas keamanan pada sistem informasi tetapi juga

membahas terkait manajemen keamanan informasi, dan cocok pada semua jenis organisasi.

Selain itu kegiatan ini akan memberikan informasi mengenai seberapa besar nilai tingkat kemampuan *(capability level)* dan tingkat kematangan *(maturity level)* serta level tingkat kemampuan *(capability level)* dan tingkat kematangan *(maturity)* keamanan sistem informasi pada UIN Raden Fatah menggunakan CMMI *(Capability Maturity Model Integration)* dengan tingkat level kemampuan (0-3) dan tingkat level kematangan (1-5).

1.2 Tujuan Audit

Adapun tujuan evaluasi tata kelola keamanan sistem informasi ini yaitu:

1. Memeriksa kondisi tata kelola keamanan sistem informasi pada UIN Raden Fatah saat ini berdasarkan standar ISO/IEC 27002:2013.
2. Mengetahui besar nilai tingkat kemampuan *(capability level)* dan nilai tingkat kematangan *(maturity level)* keamanan pada UIN Raden Fatah.

1.3 Alat dan Bahan

Alat-alat yang digunakan untuk mendukung keberhasilan evaluasi tata kelola, yaitu:

1. *Microsoft Office* : sebagai alat media tulis laporan dan pembuatan lembar kerja
2. Kamera : sebagai alat pengambilan gambar atau foto saat evaluasi
3. Alat perekam : sebagai alat pengambilan suara saat wawancara
4. Lembar kerja assessment audit: sebagai alat media pengisian data informasi saat

Jenis bahan yang digunakan untuk mendukung keberhasilan evaluasi, yaitu:

1. Bukti langsung atau tidak langsung

   Bukti langsung berupa bukti yang bersifat fakta yang dapat berupa dokumen sah terkait dengan kegiatan yang berlangsung, seperti Surat Keputusan (SK) Rektor, Surat Keputusan (SK) Kementerian Agama, dan Standard Operation Procedure (SOP). Sedangkan bukti tidak langsung berupa bukti yang tidak menggambarkan secara langsung fakta yang ada, melainkan bukti tersebut

berupa penarikan kesimpulan, seperti informasi yang didapatkan melalui proses wawancara.

2. Bukti primer atau sekunder

   Bukti primer berupa bukti yang memuat data utama yang diperlukan dalam melakukan kegiatan evaluasi, seperti data hasil pengisian lembar kerja assessment. Sedangkan bukti sekunder berupa bukti yang memuat data pendukung yang diperlukan dalam melakukan kegiatan evaluasi, seperti gambar struktur organisasi, foto, dan informasi penting dari buku dan jurnal terkait evaluasi tata kelola keamanan sistem informasi.

3. Fakta atau bukti hasil analisis

   Bukti hasil analisis yang dimaksud berupa laporan hasil audit yang memuat informasi kegiatan evaluasi tata kelola keamanan sistem informai yang sudah dilakukan, serta rekomendasi evaluator pada temuan yang belum sesuai berdasarkan ISO/IEC 27002:2013.

4. *Record* atau *Testimonial Edvidence*

   Testimonial evidence yang dimaksud adalah bukti yang didapatkan melalui alat rekam suara pada proses wawancara berlangsung.

1.4 Mekanisme Evaluasi

Mekanisme evaluasi tata kelola keamanan sistem informasi dilakukan dengan menyebarkan lembar kerja *assestmen* yang akan diisi dengan pendampingan. Lembar kerja *assestment* ini berisikan pertanyaan yang merujuk pada 14 klausul ISO/IEC 27002:2013. Setelah pengisian dilakukan, selanjutnya akan menganalisis kesesuaian antara implementasi pada UIN Raden Fatah dan implementasi berdasarkan pedoman ISO/IEC 27002:2013. Setelah melakukan analisis selanjunya akan memberikan rekomendasi yang merujuk pada pedoman ISO/IEC 27002:2013 terhadap temuan pada implementasi tata kelola yang berjalan belum sesuai dengan standar ISO/IEC 27002:2013. Selain itu akan menilai *capability level* dan *maturity level* dari setiap klausul ISO/IEC 27002:2013 agar dapat diperoleh nilai rata-rata tingkat kemampuan *(capability level)* dan tingkat kematangan *(maturity level)* untuk tata kelola keamanan sistem informasi pada UIN Raden Fatah Palembang.

BAB II
METODOLOGI

2.1 Ruang Lingkup

Adapun ruang lingkup evaluasi tata kelola keamanan sistem informasi yaitu sebagai berikut:

1. Objek : Universitas Islam Negeri Raden Fatah Palembang
2. Periode waktu : 18 Mei 2022 - 20 Juli 2022
3. Fokus narasumber:

Tabel 2.1 Narasumber

Jabatan	Klausul Pengendalian Audit	Auditee
CEO *(Chief Executive Officer)*	ISO/IEC 27002 Klausul C.5	Kepala PUSTIPD
	ISO/IEC 27002 Klausul C.8	Kepala Bagian Umum Biro AUPK
DIM *(Director Information Management)*	ISO/IEC 27002 Klausul C.7	Kasubbag Ortala Bagian Kepegawaian
	ISO/IEC 27002 Klausul C.15	Divisi Dikat PUSTIPD
CIO *(Chief Information Officer)*	ISO/IEC 27002 Klausul C.17	Pengelola Data PUSTIPD
	ISO/IEC 27002 Klausul C.18	Kepala PUSTIPD
ISO *(Information Security Officer)*	ISO/IEC 27002 Klausul C.6	Kepala PUSTIPD
	ISO/IEC 27002 Klausul C.9	Divisi Diklat PUSTIPD
	ISO/IEC 27002 Klausul C.10	Pengelola Data PUSTIPD
	ISO/IEC 27002 Klausul C.11	Pengelola Data PUSTIPD
	ISO/IEC 27002 Klausul C.12	Divisi Pengembangan *Software* PUSTIPD
	ISO/IEC 27002 Klausul C.13	Divisi Jaringan PUSTIPD
	ISO/IEC 27002 Klausul C.14	Divisi Pengembangan *Software* PUSTIPD
	ISO/IEC 27002 Klausul C.16	Divisi Pengembangan *Software* PUSTIPD

2.2 Metode Pengumpulan Data

Adapun ruang lingkup evaluasi tata kelola keamanan sistem informasi yaitu sebagai berikut:

1) Wawancara

   Cara pengumpulan data yang pertama yaitu melalui proses tanya jawab narasumber.

2) Lembar kerja *assessment*

   Cara pengumpulan data yang kedua yaitu pengisian lembar kerja assessment oleh yang terlibat dengan pendampingan.

3) Observasi

Salah satu pengumpulan data pada penelitian ini yaitu melakukan kegiatan observasi pada beberapa bagian unit kerja pada UIN Raden Fatah Palembang yaitu unit administrasi kepegawaian dan hukum, unit perencanaan dan keuangan, unit pusat teknologi dan infor Salah satu pengumpulan data pada penelitian ini yaitu melakukan kegiatan observasi pada beberapa bagian unit kerja pada UIN Raden Fatah Palembang yaitu unit administrasi kepegawaian dan hukum, unit perencanaan dan keuangan, unit pusat teknologi dan informasi pangkalan data (PUSTIPD).masi pangkalan data (PUSTIPD).

4) Studi kepustakaan

   Cara pengumpulan data pertama yaitu melakukan studi kepustakaan melalui *review* jurnal dan buku untuk menambah informasi terkait metode evaluasi yang dilakukan, dan menggunakan buku pedoman ISO/IEC 27002:2013 sebagai pedoman dalam melakukan evaluasi tata kelola keamanan sistem informasi.

5) *Browsing* Internet

   Cara pengumpulan data kedua yaitu melakukan *browsing* internet dengan menelusuri beberapa halaman *website* yang dapat menambah informasi penting terkait kebutuhan pada evaluasi ini, seperti berita acara dan dokumen online pada UIN Raden Fatah Palembang.

BAB III
HASIL ANALISIS

Berikut adalah hasil evaluasi tata kelola yang diperoleh dari kegiatan analisis evaluasi keamanan sistem informasi menggunakan ISO/IEC 27002:2013 pada UIN Raden Fatah yaitu:

1. C.5 Kebijakan keamanan informasi

Tabel 3.1 Kondisi Implementasi Kontrol Keamanan Pada C.5

Klausul	**:**	**C.5 Kebijakan keamanan informasi**
Kategori keamanan utama	**:**	**C.5.1 Arahan manajemen untuk keamanan informasi**
Implementasi saat ini		**Implementasi ISO 27002:2013**
Kontrol keamanan C.5.1.1 Kebijakan untuk keamanan informasi Terdapat kebijakan keamanan informasi berupa SOP dalam bentuk dokumen *online* dan belum diterbitkan secara formal, masih bersifat umum, dan belum lengkap berdasarkan standar kebijakan sistem manajemen keamanan informasi.		Serangkaian kebijakan untuk keamanan informasi harus ditetapkan, disetujui oleh manajemen, diterbitkan dan dikomunikasikan kepada karyawan dan pihak eksternal terkait.
Kontrol keamanan C.5.1.2 Tinjaun kebijakan untuk keamanan informasi Peninjauan kebijakan keamanan informasi pada UIN Raden Fatah dilakukan dengan menyesuaikan dinamika dan kebutuhan organisasi pada waktu tertentu, dan belum dilakukan secara berkala.		Kebijakan untuk keamanan informasi harus ditinjau pada interval yang direncanakan agar dapat memastikan kesesuaian, kecukupan, dan keefektifannya yang berkelanjutan.

2. C.6 Organisasi keamanan informasi

Tabel 3.2 Kondisi Implementasi Kontrol Keamanan Pada C.6

Klausul	**:**	**C.6 Organisasi keamanan informasi**
Kategori keamanan utama	**:**	**C.6.1 Organisasi internal** **C.6.2 Perangkat seluler dan kerja jarak jauh**
Implementasi saat ini		**Implementasi ISO 27002:2013**
Kontrol keamanan C.6.1.1 Peran dan tanggung jawab keamanan informasi Saat ini tanggung jawab keamanan informasi dikelola oleh unit Pusat Teknologi dan Pangkalan Data (PUSTIPD) dengan pengalokasian tugas yang terdiri dari 1 kepala PUSTIPD dan 3 divisi yaitu divisi diklat, divisi jaringan, dan divisi pengembangan *software*.		Semua tanggung jawab keamanan informasi harus ditetapkan dan dialokasikan.
Kontrol keamanan C.6.1.2 Pemisahan tugas Secara teknis di lapangan pemisahan tugas tidak dilakukan, karena keterbatasannya sumber daya manusia yang dimiliki, maka untuk menjalankan tugas dilakukan secara personal yaitu		Tugas dan area tanggung jawab yang saling bertentangan harus dipisahkan untuk mengurangi peluang untuk modifikasi yang tidak sah atau tidak disengaja atau penyalahgunaan aset organisasi.

dengan bergantung pada satu individu, baik dalam membuat, memelihara, dan memperbaiki aplikasi atau *website*.	
Kontrol keamanan C.6.1.3 Kontak dengan pihak berwewenang Pihak yang berwewenang dalam menanggapi insiden keamanan informasi pada UIN Raden Fatah yaitu pengelola PUSTIPD melalui divisi atau personal yang sudah ditetapkan.	Memiliki kontak yang tepat yang berwewenang dengan otoritas terkait.
Kontrol keamanan C.6.1.4 Kontak dengan kelompok minat khusus Saat ini UIN Raden Fatah belum memiliki kelompok khusus yang sangat memiliki pemahaman mengenai praktik dan lingkungan keamanan sistem informasi. Tetapi UIN Raden Fatah saat ini sudah memiliki kelompok/unit PUSTIPD, yang menjadi kelompok pengelola teknologi informasi, sehingga pemahaman praktik dan lingkungan keamanan informasi disesuaikan dengan kebutuhan keamanan sistem informasi yang ada.	Organisasi harus memiliki kelompok khusus atau forum keamanan khusus dan profesional asosiasi
Kontrol keamanan C.6.1.5 Keamanan informasi dalam manajemen proyek Penanganan keamanan informasi saat ini tidak ditangani dalam manejemen proyek, tetapi dilakukan dengan menyesuaikan dinamika dan kebutuhan di waktu yang diperlukan.	Keamanan informasi harus ditangani dalam manajemen proyek, terlepas dari apa jenis proyeknya.

Tabel 3.2 Kondisi Implementasi Kontrol Keamanan Pada C.6 Lanjutan

Klausul	**:**	**C.6 Organisasi keamanan informasi**
Kategori keamanan utama	**:**	**C.6.1 Organisasi internal** **C.6.2 Perangkat seluler dan kerja jarak jauh**
Implementasi saat ini		**Implementasi ISO 27002:2013**
Kontrol keamanan C.6.2.1 Kebijakan perangkat seluler Kebijakan keamanan pendukung dalam penggunaan perangkat seluler saa ini berupa himbauan prosedur atau aturan yang terdapat pada beberapa layanan sistem informasi tertentu.		Mengadopsi kebijakan dan langkah-langkah keamanan pendukung untuk mengelola risiko yang dikomunikasikan melalui penggunaan perangkat seluler.
Kontrol keamanan C.6.2.2 Bekerja jarak jauh Penerapan kebijakan keamanan dalam melindungi informasi jarak jauh berupa pembatasan hak akses masuk pada sistem, dan hanya dapat dilakukan oleh pemangku kepentingan saja. Tetapi kebijakan ini belum ditetapkan secara tertulis, sehingga penerapan dan langkah keamanan yang diterapkan, dilakukan dengan mengkomunikasikan kebijakan tersebut kepada pegawai.		Menerapkan kebijakan dan langkah-langkah keamanan pendukung untuk melindungi informasi yang diakses, diproses atau disimpan di situs teleworking.

3. C.7 Keamanan sumber daya manusia

Tabel 3.3 Kondisi Implementasi Kontrol Keamanan Pada C.7

Klausul	**:**	**C.7 Keamanan sumber daya manusia**
Kategori keamanan utama	**:**	**C.7.1 Sebelum bekerja** **C.7.2 Selama bekerja** **C.7.3 Pemutusan hubungan kerja dan perubahan pekerjaan**
Implementasi saat ini		**Implementasi ISO 27002:2013**
Kontrol keamanan C.7.1.1 Penyaringan Implementasi penyaringan kandidat pegawai pada UIN Raden Fatah mengikuti prosedur dan persyaratan penerimaan calon pegawai pemerintah yang terdiri dari dua kriteria posisi pegawai yaitu pegawai Aparatur Sipil Negara (ASN) dan Non Aparatur Sipil Negara (Non-ASN) sesuai dengan standar Badan Kepegawaian Negara (BKN) RI dan standar kebutuhan UIN Raden Fatah dengan mempertimbangkan tugas pokok kandidat pegawai yang diperlukan.		Melakukan pemeriksaan verifikasi latar belakang pada semua kandidat, sesuai dengan hukum, peraturan, dan etika yang relevan dan harus proporsional dengan persyaratan bisnis, klasifikasi informasi yang akan diakses dan risiko yang dirasakan.

Tabel 3.3 Kondisi Implementasi Kontrol Keamanan Pada C.7 Lanjutan

Klausul	**:**	**C.7 Keamanan sumber daya manusia**
Kategori keamanan utama	**:**	**C.7.1 Sebelum bekerja** **C.7.2 Selama bekerja** **C.7.3 Pemutusan hubungan kerja dan perubahan pekerjaan**
Implementasi saat ini		**Implementasi ISO 27002:2013**
Kontrol keamanan C.7.1.2 Syarat dan ketentuan kerja Bentuk syarat dan ketentuan bagi pegawai yang menyanggupi tanggung jawabnya untuk tugas pokok yang diterimanya dinyatakan dalam bentuk perjanjian kontrak pegawai. Perjanjian kontrak pegawai ini terbagi menjadi: - Surat Keputusan (SK) dari Kementerian Agama Republik Indonesia. - Surat Keputusan (SK) dari Rektor UIN Raden Fatah yang berlaku selama 1 tahun. - Surat perjanjian kerja		Perjanjian kontrak dengan pegawai dan kontraktor harus menyatakan mereka dan organisasi tanggung jawab untuk keamanan informasi.
Kontrol keamanan C.7.2.1 Tanggung jawab manajemen UIN Raden Fatah menghimbau untuk setiap pegawai, dosen, dan staff mengikuti prosedur keamanan informasi yang dilampirkan pada kebijakan atau SOP yang sudah dibuat.		Manajemen harus mewajibkan semua pegawai dan kontraktor untuk menerapkan keamanan informasi sesuai dengan kebijakan dan prosedur yang ditetapkan organisasi.
Kontrol keamanan C.7.2.2 Kesadaran, pendidikan, dan pelatihan keamanan Fasilitas pelatihan keamanan informasi pada UIN Raden Fatah diberikan oleh		Semua pegawai organisasi harus menerima kesadaran, pendidikan dan pelatihan dan pembaruan rutin dalam kebijakan dan prosedur

pihak PUSTIPD dalam bentuk pelatihan dan pengajaran. Selain itu dapat juga melalui DIKLAT dari pihak yang berkaitan langsung dengan sistem informasi yang digunakan, seperti himbauan untuk mengikuti SOP keamanan sistem informasi dan lain sebagainya. Namun saat ini untuk SOP yang ada tidak dilakukan pembaruan atau peninjauan secara berkala, melainkan hanya dilakukan pembaruan jika dibutuhkan saja. Sehingga dalam pelaksanaan pelatihan dan pembelajaran tidak dilakukan secara berkala.	organisasi, yang relevan untuk fungsi pekerjaan mereka.
Kontrol keamanan C.7.2.3 Proses pendisiplinan UIN Raden Fatah memberikan proses disipliner formal terhadap pegawai, dosen, maupun staff dengan mengikuti Tata Cara Penjatuhan Disiplin (PP 94 Tahun 2021). UIN Raden Fatah memberikan sanksi dengan 3 tingkat kriteria yaitu pertama berbentuk peneguran secara lisan dan surat, kedua berbentuk peneguran dalam penurunan gaji, dan ketiga yaitu diberhentikan.	Harus ada proses disipliner formal dan dikomunikasikan untuk mengambil tindakan terhadap pegawai yang telah melakukan pelanggaran keamanan informasi
Kontrol keamanan C.7.3.1 Pemutusan atau perubahan tanggung jawab pekerja Dalam pemutusan atau perubahan tanggung jawab pekerjaan, UIN Raden Fatah tetap menentukan tanggung jawab dan tugas keamanan informasi yang berlaku sebelumnya, agar dapat disesuaikan dan dikomunikasian dengan pegawai yang menggantikan. Maka dari itu tanggung jawab dan tugas tersebut dapat diterapkan oleh pegawai yang disertai dengan pemberian surat perjanjian kerja.	Menentukan, mengkomunikasikan, dan menegakkan kepada pegawai pegganti, mengenai tanggung jawab dan tugas keamanan informasi yang tetap berlaku setelah adanya penghentian atau perubahan pekerjaan pegawai.

4. C.8 Manajemen aset

Tabel 3.4 Kondisi Implementasi Kontrol Keamanan Pada C.8

Klausul	**:**	**C.8 Manajemen aset**
Kategori keamanan utama	**:**	**C.8.1 Tanggung jawab atas aset** **C.8.2 Klasifikasi informasi** **C.8.3 Penanganan media**
Implementasi saat ini		**Implementasi ISO 27002:2013**
Kontrol keamanan C.8.1.1 Invetaris aset UIN Raden Fatah melakukan identifikasi terhadap aset informasi dan fasilitas pemprosesan aset yang dimiliki melalui kegiatan evaluasi. Pendataan (inventarisasi) aset informasi maupun aset fasilitas pemprosesan informasi sudah terdokumentasi secara otomatis pada sistem. UIN Raden Fatah juga melakukan pemeliharaan dengan		Mengidentifikasi dan mendokumentasikan aset yang relevan dalam siklus hidup informasi organisasi, yang mencakup pembuatan, pemrosesan, penyimpanan, transmisi, penghapusan dan kehancuran. Dokumentasi harus dipelihara dalam inventaris khusus sebagaimana mestinya.

menerapkan sistem pencadangan data sebagai bentuk pemeliharaan aset informasi, sedangkan bentuk pemeliharaan aset fasilitas pemprosesan informasi dilakukan dengan *service* melalui kerjasama bersama vendor yang disesuaikan dengan jenis asetnya.	
Kontrol keamanan C.8.1.2 Kepemilikan aset Saat ini pada UIN Raden Fatah setiap aset informasi yang terdokumentasi dalam inventarisasi aset dimiliki dan dikelola oleh masing-masing penanggung jawab aset.	Tanggung jawab kepemilikan terhadap aset yang disimpan dalam inventarisasi aset.
Kontrol keamanan C.8.1.3 Penggunaan aset yang dapat diterima Dalam penggunaan aset informasi dan fasilitas pemprosesan informasi UIN Raden Fatah menerapkan aturan atau prosedur yang dibuat dalam SOP. - SOP Penggunaan dan operasional ruang server. - SOP Layanan peminjaman barang.	Mengidentifikasi, mendokumentasi, dan mengimplementasi aturan untuk penggunaan informasi dan aset yang dapat diterima baik berupa informasi maupun fasilitas pengolahan informasi.
Kontrol keamanan C.8.1.4 Pengembalian aset Jika terdapat pemutusan hubungan kerja pada UIN Raden Fatah, aset akan dikembalikan kepada masing-masing bagian unit pegawai atau pihak ketiga bekerja, dan selanjutnya aset tersebut akan digunakan kembali oleh pegawai baru atau pihak ketiga pengganti.	Semua karyawan dan pengguna pihak eksternal harus mengembalikan semua aset organisasi yang mereka miliki pada saat pemutusan hubungan kerja, kontrak atau perjanjian mereka.

Tabel 3.4 Kondisi Implementasi Kontrol Keamanan Pada C.8 Lanjutan

Klausul	**:**	**C.8 Manajemen aset**
Kategori keamanan utama	**:**	**C.8.1 Tanggung jawab atas aset** **C.8.2 Klasifikasi informasi** **C.8.3 Penanganan media**
Implementasi saat ini		**Implementasi ISO 27002:2013**
Kontrol keamanan C.8.2.1 Klasifikasi informasi Aset informasi pada UIN Raden Fatah disimpan sesuai dengan tingkat kerahasiaannya melalui pembatasan hak akses masuk berdasarkan tipe pengguna.		Informasi harus diklasifikasikan dalam hal persyaratan hukum, nilai, kekritisan dan kepekaan terhadap pengungkapan atau modifikasi yang tidak sah.
Kontrol keamanan C.8.2.2 Pelabelan informasi Penerapan serangkaian prosedur dalam pelabelan informasi mengacu pada prosedur negara dengan memberikan label atau nomor seri yang ditempel pada bagian aset yang disertai dengan barcode label aset.		Serangkaian prosedur yang tepat untuk pelabelan informasi harus dikembangkan dan diimplementasikan dalam sesuai dengan skema klasifikasi informasi yang diadopsi oleh organisasi.
Kontrol keamanan C.8.2.3 Penanganan aset		Prosedur penanganan aset harus dikembangkan dan diterapkan sesuai dengan informasi skema klasifikasi yang diadopsi oleh organisasi.

Penanganan aset pada UIN Raden Fatah mengacu pada prosedur negara, baik dalam pengadaan dan penerimaan barang, pelabelan, maupun penghapusan barang.	
Kontrol keamanan C.8.3.1 Manajemen media yang dapat dipindahkan Prosedur pemindahan media dilakukan dengan mencadangkan data pada sitem, sehingga pada aset yang baru data informasi pada data informasi dapat dipulihkan kembali.	Prosedur harus diterapkan untuk pengelolaan media yang dapat dipindahkan sesuai dengan skema klasifikasi yang diadopsi oleh organisasi.
Kontrol keamanan C.8.3.2 Pembuangan media Prosedur yang digunakan untuk menghilangkan media berbentuk barang mengikuti prosedur negara. Namun dalam pembuangan media berbetuk data belum terdapat aturan tertentu dalam pelaksanaannya, sehingga menyesuaikan kebutuhan yang diperlukan saja.	Membuang media yang tidak diperlukan lagi denga naman, dan menggunakan prosedur formal.
Kontrol keamanan C.8.3.3 Transfer media Saat ini pada UIN Raden Fatah sudah terdapat tim khusus pengelola sarana dan prasarana yang berwewenang dalam memeriksa fisik media saat pengantaran media. Namun belum terdapat proses khusus dalam melindungi fisik media saat terjadinya transfer media.	Media yang berisi informasi harus dilindungi dari akses yang tidak sah dan penyalahgunaan aset.

5. C.9 Kontrol akses

Tabel 3.5 Kondisi Implementasi Kontrol Keamanan Pada C.9

Klausul	**:**	**C.9 Kontrol akses**
Kategori keamanan utama	**:**	**C.9.1 Persyaratan bisnis untuk kontrol akses** **C.9.2 Manajemen akses pengguna** **C.9.3 Tanggung jawab pengguna** **C.9.4 Kontrol akses sistem dan aplikasi**
Implementasi saat ini		**Implementasi ISO 27002:2013**
Kontrol keamanan C.9.1.1 Kebijakan kontrol akses Kebijakan kontrol akses pada UIN Raden Fatah sudah ditetapkan, tetapi belum secara formal dalam dokumen khusus yang termuat dalam SOP dan Blueprint pengembangan TIK. Selain itu proses peninjauan dilakukan dengan menyesuaikan organisasi yang sesuai dengan syarat keamanan informasi.		Kebijakan kontrol akses harus ditetapkan, didokumentasikan dan ditinjau berdasarkan bisnis dan persyaratan keamanan informasi.
Kontrol keamanan C.9.1.2 Akses ke jaringan dan layanan jaringan Hak akses jaringan maupun layanan jaringan pada UIN Raden Fatah dibatasi berdasarkan tipe pengguna.		Pengguna hanya boleh diberikan akses ke jaringan dan layanan jaringan yang telah mereka miliki khusus diizinkan untuk digunakan.

Kontrol keamanan C.9.2.1 Pendaftaran dan pembatalan pendaftaran pengguna Pendaftaran pengguna hak akses pada UIN Raden Fatah dilakukan melalui pengajuan dari calon pengguna untuk dibuatkan akun.	Proses registrasi dan de-registrasi pengguna formal harus diterapkan untuk memungkinkan penugasan hak akses.
Kontrol keamanan C.9.2.2 Penyediaan akses pengguna Proses penyediaan akses pengguna dapat dilakukan dengan mengajukan pembuatan akun user kepada pihak PUSTIPD. Sedangkan pencabutan hak akses dapat dilakukan saat terdapat mahasiswa, pegawai, staf atau dosen yang sudah tidak berkuliah/berkerja di UIN Raden Fatah. Akses yang dicabut seperti layanan email UIN Raden Fatah, dan aplikasi-aplikasi tertentu.	Proses penyediaan akses pengguna formal harus diterapkan untuk menetapkan atau mencabut hak akses untuk semua jenis pengguna ke semua sistem dan layanan.
Kontrol keamanan C.9.2.3 Manajemen hak akses istimewa Pengendalian hak akses pengguna dan hak akses istimewa pada UIN Raden Fatah dilakukan oleh unit PUSTIPD. Penggunaan hak akses istimewa dibatasi dengan beberapa unit tertetu yang membutuhkan hak akses dengan memberikan akses melalui VPN (akses jaringan).	Membatasi dan mengendalikan alokasi dan penggunaan hak akses istimewa.

Tabel 3.5 Kondisi Implementasi Kontrol Keamanan Pada C.9 Lanjutan

Klausul	**:**	**C.9 Kontrol akses**
Kategori keamanan utama	**:**	**C.9.1 Persyaratan bisnis untuk kontrol akses** **C.9.2 Manajemen akses pengguna** **C.9.3 Tanggung jawab pengguna** **C.9.4 Kontrol akses sistem dan aplikasi**
Implementasi saat ini		**Implementasi ISO 27002:2013**
Kontrol keamanan C.9.2.4 Pengelolaan informasi otentikasi rahasia pengguna Proses pengalokasian informasi otentikasi rahasia belum dilakukan secara formal, dan hanya dilakukan dengan menyesuaikan kebutuhan dan *by accident.*		Alokasi informasi otentikasi rahasia harus dikontrol melalui formal proses manajemen.
Kontrol keamanan C.9.2.5 Tinjauan hak akses penggun Peninjauan hak akses pada UIN Raden Fatah dilakukan dengan menyesuaikan kebutuhan organisasi, dan tidak dilakukan secara berkala.		Pemilik aset harus meninjau hak akses pengguna secara berkala.
Kontrol keamanan C.9.2.6 Penghapusan atau penyesuaian hak akses Implementasi yang dilakukan UIN Raden Fatah dalam penghapusan atau penyesuaian hak akses yaitu dengan menghapus hak akses pengguna, seperti		Hak akses semua karyawan dan pengguna pihak eksternal terhadap informasi dan pemrosesan informasi fasilitas harus dihapus pada saat pemutusan hubungan kerja, kontrak atau perjanjian, atau disesuaikan dengan perubahan.

email UIN Raden Fatah dan aplikasi-aplikasi tertentu.	
Kontrol keamanan C.9.3.1 Penggunaan informasi otentikasi rahasia Penggunaan informasi otentikasi rahasia pada UIN Raden Fatah dilakukan berdasarkan himbauan yang diberikan pada dashboard website pengguna.	Pengguna harus diminta untuk mengikuti praktik organisasi dalam penggunaan informasi otentikasi rahasia.
Kontrol keamanan C.9.4.1 Pembatasan akses informasi Pembatasan akses informasi pada UIN Raden Fatah dilakukan dan disesuaikan berdasarkan tipe pengguna.	Akses ke informasi dan fungsi sistem aplikasi harus dibatasi sesuai dengan: kebijakan kontrol akses.
Kontrol keamanan C.9.4.2 Prosedur login yang aman Prosedur log-on yang aman pada UIN Raden Fatah sudah di implementasikan pada setiap website yang UIN Raden Fatah.	Jika disyaratkan oleh kebijakan kontrol akses, akses ke sistem dan aplikasi harus dikontrol oleh prosedur log-on yang aman.
Kontrol keamanan C.9.4.3 Sistem manajemen kata sandi Manajemen kata sandi pada website tertentu sudah dilengkapi dengan fitur capta saat login.	Sistem manajemen kata sandi harus interaktif dan harus memastikan kata sandi berkualitas.

Tabel 3.5 Kondisi Implementasi Kontrol Keamanan Pada C.9 Lanjutan

Klausul	**:**	**C.9 Kontrol akses**
Kategori keamanan utama	**:**	**C.9.1 Persyaratan bisnis untuk kontrol akses** **C.9.2 Manajemen akses pengguna** **C.9.3 Tanggung jawab pengguna** **C.9.4 Kontrol akses sistem dan aplikasi**
Implementasi saat ini		**Implementasi ISO 27002:2013**
Kontrol keamanan C.9.4.4 Penggunaan program utilitas istimewa Program utilitas yang dimiliki pada UIN Raden Fatah antara lain dashboard, utilitas prosesor, dan network pengguna.		Penggunaan program utilitas yang mungkin mampu mengesampingkan kontrol sistem dan aplikasi harus dibatasi dan dikontrol dengan ketat.
Kontrol keamanan C.9.4.5 Kontrol akses ke kode sumber program Kontrol akses ke kode sumber program untuk setiap sistem informasi yang ada pada UIN Raden Fatah dikendalikan oleh unit PUSTIPD.		Memberikan pembatasan akses ke kode sumber program.

6. C.10 Kriptografi

Tabel 3.6 Kondisi Implementasi Kontrol Keamanan Pada C.10

Klausul	**:**	**C.10 Kriptografi**
Kategori keamanan utama	**:**	**C.10.1 Kontrol kriptografi**
Implementasi saat ini		**Implementasi ISO 27002:2013**
Kontrol keamanan C.10.1.1 Kebijakan penggunaan kontrol kriptografi Kebijakan prosedur maupun aturan pengembangan tentang penggunaan kontrol kriptografi dalam perlindungan informasi belum ada, sehingga dilakukan berdasarkan himbauan yang langsung pada pelaksanaan teknis penggunaan penggunaan enkripsi pada setiap sistem informasi yang disesuaikan dengan kebutuhan keamanan sistem informasi tersebut.		Kebijakan tentang penggunaan kontrol kriptografi untuk perlindungan informasi harus dikembangkan dan dilaksanakan.
Kontrol keamanan C.10.1.2 Manajemen kunci Kebijakan prosedur maupun aturan manajemen kunci kriptografi baik dalam penggunaan kunci, perlindungan kunci, pengembangan kebijakan kunci, maupun masa pakai kunci belum ada. Implementasi yang dilakukan saat ini hanya berdasarkan himbauan yang langsung pada pelaksanaan teknis penggunaan penggunaan enkripsi pada setiap sistem informasi yang disesuaikan dengan kebutuhan keamanan sistem informasi tersebut.		Kebijakan tentang penggunaan, perlindungan, dan masa pakai kunci kriptografi harus dikembangkan dan diimplementasikan melalui seluruh siklus hidup mereka.

7. C.11 Keamanan fisik dan lingkungan

Tabel 3.7 Kondisi Implementasi Kontrol Keamanan Pada C.11

Klausul	**:**	**C.11 Keamanan fisik dan lingkungan**
Kategori keamanan utama	**:**	**C.11.1 Area aman** **C.11.2 Peralatan**
Implementasi saat ini		**Implementasi ISO 27002:2013**
Kontrol keamanan C.11.1.1 Perimeter keamanan fisik Memberikan perlindungan terhadap area yang terdapat fasilitas yang sensitif, dengan menyediakan lingkungan yang dilengkapi sensor *kide fire system* otomatis, sensor akses pintu X302-S otomatis, mesin absensi, CCTV, dan sensor suhu ruangan.		Perimeter keamanan harus ditentukan dan digunakan untuk melindungi area yang mengandung sensitif atau kritis fasilitas pengolahan informasi dan informasi.
Kontrol keamanan C.11.1.2 Kontrol entri fisik Saat ini dalam kontrol entri fisik pada UIN Raden Fatah, akses masuk ke dalam area perangkat sistem informasi (ruang *server* dan data *center*), hanya dimiliki oleh pengelola PUSTIPD, dan orang umum yang sudah memiliki izin dan		Area aman harus dilindungi oleh kontrol masuk yang sesuai untuk memastikan bahwa hanya personel yang berwenang diperbolehkan akses.

berkepentingan saja, seperti yang sudah tertera pada SOP yang sudah dibuat.	
Kontrol keamanan C.11.1.3 Mengamankan kantor, ruangan, dan fasilitas Pengamanan kantor, ruangan dan fasilitas pengelolaan informasi pada UIN Raden Fatah, sudah dilengkapi dengan fasilitas: - Proyektor dan monitor ISDB pada ruangan data center sangat membantu pengelolaan informasi pada UIN Raden Fatah, - Sensor suhu dapat membantu kestabilan suhu ruangan sehinggan alat elektronik dan perangkat sistem informasi pada ruangan data center tidak panas - Sensor akses pintu untuk mendeteksi kondisi pintu dalam keadaan terbuka atau tertutup melalui bunyi alarm pemberitahuan	Keamanan fisik untuk kantor, ruangan dan fasilitas harus dirancang dan diterapkan.
Kontrol keamanan C.11.1.4 Melindungi dari ancaman dari eksternal dan lingkungan Perlindungan fisik terhadap ancaman eksternal yang diterapkan yaitu sensor akses pintu untuk mendeteksi kondisi pintu dalam keadaan terbuka atau tertutup melalui bunyi alarm pemberitahuan dan k*ide fire system* (alat pemadam kebakaran otomatis). Penerapan sensor akses pintu *kide fire system* ini diterapkan oleh pengelola ruang server atua data center PUSTIPD UIN Raden Fatah melalui sistem *finger print*.	Perlindungan fisik terhadap bencana alam, serangan berbahaya atau kecelakaan harus dirancang dan diterapkan.

Tabel 3.7 Kondisi Implementasi Kontrol Keamanan Pada C.11 Lanjutan

Klausul	**:**	**C.11 Keamanan fisik dan lingkungan**
Kategori keamanan utama	**:**	**C.11.1 Area aman** **C.11.2 Peralatan**
Implementasi saat ini		**Implementasi ISO 27002:2013**
Kontrol keamanan C.11.1.5 Bekerja di daerah aman Sudah dibuat dan diterapkan *Standard Operating Procedure* (SOP) Penggunaan Dan Operasional Ruang Server atau data center dalam pengelolaan informasi UIN Raden Fatah pada ruangan server dan data center PUSTIPD.		Prosedur untuk bekerja di area aman harus dirancang dan diterapkan.
Kontrol keamanan C.11.1.6 Area pengiriman dan pemuatan Secara fisik pembatasan hak akses masuk dilengkapi dengan sistem finger print yang hanya dimiliki oleh pengelola ruang server dan data center PUSTIPD, sehingga hak akses masuk bagi orang ketiga hanya diperbolehkan dengan		Titik akses seperti area pengiriman dan pemuatan dan titik lain di mana orang yang tidak berwenang dapat memasuki tempat harus dikontrol dan, jika mungkin, diisolasi dari fasilitas pemrosesan informasi untuk menghindari akses yang tidak sah.

perizinan dan pendampingan dari pengelola ruang server dan data center PUSTIPD.	
Kontrol keamanan C.11.2.1 Penampatan dan perlindungan peralatan Penempatan dan perlindungan peralatan pengelolaan informasi pada UIN Raden Fatah dilakukan dengan memposisikan letak ruangan server dan data center PUSTIPD pada lantai 4 Gedung Perpustakaan UIN Raden Fatah agar dapat terhindar dari ancaman lingkungan, seperti banjir, dan jangkauan mahasiswa, dosen, maupun pegawai UIN Raden Fatah. Sedangkan dalam melindungi dan meminimalisir ancaman dan bahaya lingkungan, UIN Raden Fatah menerapkan sensor suhu rungan dan fire system otomatis pada lingkungan pengelolaan informasi.	Peralatan harus ditempatkan dan dilindungi untuk mengurangi risiko dari ancaman dan bahaya lingkungan, dan peluang untuk akses yang tidak sah.
Kontrol keamanan C.11.2.2 Utilitas pendukung Saat ini dalam meminimalisir ancaman keamanan sistem informasi dari kegagalan daya dan gangguan lain yaitu dengan menyediakan batre cadangan dan genset.	Peralatan harus dilindungi dari kegagalan daya dan gangguan lain yang disebabkan oleh kegagalan dalam utilitas pendukung.
Kontrol keamanan C.11.2.3 Keamanan kabel Penerapan yang dilakukan jalur telekomunikasi melalui metode tanam yang dilakukan sejak pembangunan gedung UIN Raden Fatah, hal ini bertujuan untuk mengurangi resiko kerusakan akibat aktivitas manusia.	Kabel listrik dan telekomunikasi yang membawa data atau layanan informasi pendukung harus: dilindungi dari intersepsi, gangguan atau kerusakan.
Kontrol keamanan C.11.2.4 Pemeliharaan peralatan Upaya yang dilakukan UIN Raden Fatah dalam pemeliharaan peralatan yaitu dengan melakukan kegiatan monitoring atau pemantauan dan pemberian aktivasi virus.	Peralatan harus dipelihara dengan benar untuk memastikan ketersediaan dan integritasnya yang berkelanjutan.

Tabel 3.7 Kondisi Implementasi Kontrol Keamanan Pada C.11 Lanjutan

Klausul	**:**	**C.11 Keamanan fisik dan lingkungan**
Kategori keamanan utama	**:**	**C.11.1 Area aman** **C.11.2 Peralatan**
Implementasi saat ini		**Implementasi ISO 27002:2013**
Kontrol keamanan C.11.2.5 Penghapusan aset Aturan yang diterapkan UIN Raden Fatah dalam penghapusan aset yaitu dengan tidak mengizinkan peralatan sistem informasi dibawa ke luar lokasi tanpa izin dan jika dibutuhkan saja.		Peralatan, informasi, atau perangkat lunak tidak boleh dibawa ke luar lokasi tanpa izin sebelumnya.

Kontrol keamanan C.11.2.6 Keamanan peralatan dan aset di luar lokasi Upaya yang dilakukan UIN Raden Fatah dalam menangani keamanan peralatan dan aset di luar lokasi, yaitu dengan membatasi hak akses masuk pengguna.	Keamanan harus diterapkan pada aset di luar lokasi dengan mempertimbangkan berbagai risiko bekerja di luar tempat organisasi.
Kontrol keamanan C.11.2.7 Pembuangan atau penggunaan kembali peralatan secara aman Belum terdapat pembuangan peralatan yang dilakukan, sehingga peralatan tersebut masih disimpan oleh pihak PUSTIPD.	Semua item peralatan yang berisi media penyimpanan harus diverifikasi untuk memastikan bahwa setiap data sensitif dan perangkat lunak berlisensi telah dihapus atau ditimpa dengan aman sebelum dibuang atau digunakan kembali.
Kontrol keamanan C.11.2.8 Peralatan pengguna tanpa pengawasan Perlindungan peralatan tanpa pengawasan diterapkan melalui penggunaan password pada perangkat komputer atau laptop pengelola informasi.	Pengguna harus memastikan bahwa peralatan yang tidak dijaga memiliki perlindungan yang sesuai.
Kontrol keamanan C.11.2.9 Bersihkan meja dan kebijakan layer yang jelas Penerapan yang dilakukan UIN Raden Fatah dalam kebijakan *clear desk* yaitu: - Membuat jadwal kegiatan clear desk yang diarahkan langsung oleh kepala PUSTIPD - Membersihkan kondisi meja kerja setelah digunakan sebelum pulang Sedangkan penerapan yang dilakukan UIN Raden Fatah dalam kebijakan *clear screen* yaitu: - Mengeluarkan semua menu yang dibuka sebelum meninggalkan *laptop*/komputer. - Setting sleep/off power perangkat sebelum meninggalkan tempat kerja. - Memberikan *password* terhadap perangkat yang rentan terhadap aset yang penting.	Memiliki kebijakan *cleardesk* dan *clearscreen*.

8. C.12 Operasi keamanan

Tabel 3.8 Kondisi Implementasi Kontrol Keamanan Pada C.12

Klausul	**:**	**C.12 Operasi keamanan**
Kategori keamanan utama	**:**	**C.12.2 Perlindungan dari malware** **C.12.3 Cadangan** **C.12.4 Pencatatan dan pemantauan** **C.12.5 Kontrol perangkat lunak operasional** **C.12.6 Manajemen kerentanan teknis** **C.12.7 Pertimbangan audit sistem informasi**
Implementasi saat ini		**Implementasi ISO 27002:2013**
Kontrol keamanan C.12.1.1 Prosedur operasi terdokumentasi Dokumentasi prosedur operasi keamanan pada UIN Raden Fatah dibuat dalam bentuk Standard Operation Procedure (SOP). Prosedur operasi tersebut sudah tersedia bagi pengguna		Prosedur operasi harus didokumentasikan dan tersedia untuk semua pengguna yang membutuhkannya.

yang dimuat dalam bentuk (SOP) dan tersedia pada website pustipd.radenfatah.ac.id.	
Kontrol keamanan C.12.1.2 Manajemen perubahan Bentuk pengendalian terhadap manajemen perubahan pada UIN Raden Fatah yaitu: a. Bentuk pengendalian terhadap perubahan organisasi yang dilakukan oleh UIN Raden Fatah berupa revisi kebijakan operasional hanya jika diperlukan perubahan. b. Bentuk pengendalian terhadap proses bisnis yang dilakukan oleh UIN Raden Fatah berupa kerjasama dengan kontraktor (pihak ketiga) yang berkaitan dengan penunjang kebutuhan keamanan sistem informasi. c. Bentuk pengendalian terhadap fasilitas pemprosesan data pada UIN Raden Fatah berupa upaya pemeliharaan terhadap aset yang digunakan dalam pemprosesan informasi, dan memberikan alat pengaman dalam lingkungan fasilitas pemprosesan informasi. d. Bentuk pengendalian terhadap sistem yang mempengaruhi keamanan informasi pada UIN Raden Fatah berupa upaya pencadangan data informasi pada sistem informasi.	Perubahan pada organisasi, proses bisnis, fasilitas pemrosesan informasi dan sistem yang mempengaruhi keamanan informasi harus dikendalikan.
Kontrol keamanan 12.1.3 Manajemen kapasitas Dalam proses manajemen kapasitas sumber daya yang dimiliki, belum dilakukan pemantauan secara berkala, sehingga penentuan sumber daya yang dibutuhkan baik SDM maupun barang ditentukan dan disediakan berdasarkan kebutuhan saat itu. Setelah sumber daya tersedia, maka selanjutnya akan dilakukan penyetelan oleh pihak PUSTIPD melalui monitoring, namun hal ini dilakukan dalam waktu satu kali, dan akan dilakukan kembali penyetelan apabila terdapat kendala dan kebutuhan pada saat itu.	Penggunaan sumber daya harus dipantau, disetel, dan dibuat proyeksi kebutuhan kapasitas di masa mendatang untuk memastikan kinerja sistem yang diperlukan.

Tabel 3.8 Kondisi Implementasi Kontrol Keamanan Pada C.12 Lanjutan

Klausul	**:**	**C.12 Operasi keamanan**
Kategori keamanan utama	**:**	**C.12.2 Perlindungan dari malware** **C.12.3 Cadangan** **C.12.4 Pencatatan dan pemantauan** **C.12.5 Kontrol perangkat lunak operasional** **C.12.6 Manajemen kerentanan teknis** **C.12.7 Pertimbangan audit sistem informasi**
Implementasi saat ini		**Implementasi ISO 27002:2013**
Kontrol keamanan C.12.1.4 Pemisahan lingkungan pengembangan, pengujian, dan operasional		Lingkungan pengembangan, pengujian, dan operasional harus dipisahkan untuk mengurangi

Sudah terdapat unit tersendiri yang mengatur IT pada UIN Raden Fatah, yaitu unit PUSTIPD. Kondisi yang berjalan saat ini pada PUSTIPD sudah dibagi beberapa divisi pengelola sistem informasi pada UIN Raden Fatah. Namun secara implementasinya pengembangan, pengujian, dan operasional dilakukan secara personal, dimana ketiga proses tersebut dikendalikan oleh satu orang.	risiko akses tidak sah atau perubahan lingkungan operasional.
Kontrol keamanan C.12.2.1 Kontrol terhadap malware Saat ini UIN Raden Fatah memiliki kontrol deteksi yang bersifat otomatis berupa *firewall*, serta terdapat notif pemberitahuan jika terdapat ancaman *malware*. Upaya UIN Raden Fatah dalam pencegahan dari *malware* berupa penggunaan *firewal*l pada jaringan, sedangkan dari pengembangan aplikasi, lebih diperhatikannya keamanan aplikasi yang dibuat. Sedangkan bentuk pemulihan yang terapkan UIN Raden Fatah berupa penggunaan *server* HCI, sehingga terdapat snap pencadangan data yang dilakukan setiap minggu.	Kontrol deteksi, pencegahan, dan pemulihan untuk melindungi dari malware harus diterapkan, dikombinasikan dengan kesadaran pengguna yang tepat.
Kontrol keamanan C.12.3.1 Cadangan informasi a. Pencadangan dilakukan secara berkala terhadap sistem informasi tertentu saja, tetapi pada *restore* yang disertai pengujian pencadangan bagus atau tidak belum dilakukan. Sistem yang diterapkan yaitu pihak PUSTIPD percaya dengan pencadangan data yang sudah dilakukan dan apabila terdapat kejadian ancaman keamanan, maka cadangan data tersebut akan dipakai. b. Pengambilan dan pengujian perangkat lunak hanya sekali, dan akan dilakukan kembali jika diperlukan saja.	Salinan cadangan informasi, perangkat lunak, dan gambar sistem harus diambil dan diuji secara teratur di sesuai dengan kebijakan cadangan yang disepakati.

Tabel 3.8 Kondisi Implementasi Kontrol Keamanan Pada C.12 Lanjutan

Klausul	**:**	**C.12 Operasi keamanan**
Kategori keamanan utama	**:**	**C.12.2 Perlindungan dari malware** **C.12.3 Cadangan** **C.12.4 Pencatatan dan pemantauan** **C.12.5 Kontrol perangkat lunak operasional** **C.12.6 Manajemen kerentanan teknis** **C.12.7 Pertimbangan audit sistem informasi**

Implementasi saat ini	Implementasi ISO 27002:2013
Kontrol keamanan C.12.4.1 Pencatatan peristiwa a. Penerapan log peristiwa yang diterapkan secara teratur dilakukan pada aktivitas-aktivitas penting seperti log aktivitas login, log aktivitas pembayaran pada link setiap bank, dan aktivitas perubahan nilai mahasiswa. b. Belum ada penghapusan pencatatan peristiwa log aktivitas, namun sebenarnya penyimpanan pencatatan peristiwa akan terus dilakukan atau tidak tergantung pada kapasitas pada server yang dimiliki. c. Pencatatan pristiwa log pada UIN Raden Fatah belum ada yang dihapus, dan apabila server sudah melebihi kapasitas, PUSTIPD akan melakukan pencadangan data terlebih dahulu.	Log peristiwa yang merekam aktivitas pengguna, pengecualian, kesalahan, dan peristiwa keamanan informasi harus diproduksi, disimpan dan ditinjau secara teratur.
Kontrol keamanan C.12.4.2 Perlindungan informasi log Saat ini pada UIN Raden Fatah hak akses logging hanya dapat dilakukan oleh pihak PUSTIPD, sehingga tidak sembarangan orang dapat melakukan aktivitas logging.	Fasilitas logging dan informasi log harus dilindungi dari gangguan dan akses yang tidak sah.
Kontrol keamanan C.12.4.3 Log administarator dan operator Akses masuk administrator sistem serta operator sistem tercatat pada database sistem informasi. Bentuk keamanan yang diberikan berupa pemberian *password*, dan pembatasan hak akses yang hanya dapat dilakukan oleh pihak terkait. Namun akses masuk administrator sistem serta operator sistem tidak dilakukan peninjauan secara berkala, dan peninajaun dilakukan jika hanya terdapat permasalahan yang mengancam keamanan sistem informasi.	Administrator sistem dan aktivitas operator sistem harus dicatat dan log dilindungi dan ditinjau secara teratur.
Kontrol keamanan C.12.4.4 Sinkronisasi jam Saat ini pada UIN Raden Fatah waktu pemprosesan informasi Semua disesuaikan dan merujuk pada waktu WIB.	Jam dari semua sistem pemrosesan informasi yang relevan dalam organisasi atau domain keamanan harus disinkronkan ke sumber waktu referensi tunggal.

Tabel 3.8 Kondisi Implementasi Kontrol Keamanan Pada C.12 Lanjutan

Klausul	**:**	**C.12 Operasi keamanan**
Kategori keamanan utama	**:**	**C.12.2 Perlindungan dari malware** **C.12.3 Cadangan** **C.12.4 Pencatatan dan pemantauan** **C.12.5 Kontrol perangkat lunak operasional** **C.12.6 Manajemen kerentanan teknis** **C.12.7 Pertimbangan audit sistem informasi**

Implementasi saat ini	Implementasi ISO 27002:2013
Kontrol keamanan C.12.5.1 Instalasi perangkat lunak operasional Saat ini UIN Raden Fatah belum memiliki jenis aplikasi yang memerlukan prosedur khusus dalam intalasi pada PC. Saat ini UIN hanya memiliki aplikasi mobile yang dapat di *donwload* melalui *playstore* yang tidak memerlukan prosedur instalasi khusus. Sehingga UIN Raden Fatah belum memilki prosedur khusus instalasi perangkat lunak.	Prosedur harus diterapkan untuk mengontrol instalasi perangkat lunak pada sistem operasional.
Kontrol keamanan C.12.6.1 Manajemen kerentenan teknis a. Informasi kerentanan teknis dari sistem informasi yang digunakan akan diperoleh dari pengguna, sehingga pihak PUSTIPD akan mendapatkan informasi kerentanan tersebut setelah pengguna menggunakan sistem tersebut. Maka dari itu perolehan informasi tersebut tidak tepat waktu. Setelah masalah didapatkan, kemudian pihak PUSTIPD akan segera memperbaiki kerentanan sistem yang bermasalah tersebut. b. Saat ini UIN Raden Fatah sudah memiliki SOP nya sendiri yaitu SOP pelayanan penerimaan laporan masalah IT yang dapat di akses pada *website* PUSTIPD.	Informasi tentang kerentanan teknis dari sistem informasi yang digunakan harus diperoleh dalam tepat waktu, eksposur organisasi terhadap
Kontrol keamanan C.12.6.2 Pembatasan intalasi perangkat lunak Saat ini UIN Raden Fatah belum memiliki jenis sistem informasi yang memerlukan aturan khusus dalam intalasi. Saat ini UIN hanya memiliki aplikasi mobile yang bisa di *donwload* melalui *playstore* yang tidak memerlukan aturan instalasi khusus.	Aturan yang mengatur instalasi perangkat lunak oleh pengguna harus ditetapkan dan diimplementasikan.
Kontrol keamanan C.12.7.1 Pengendalian audit sistem informasi Pertimbangan yang diberikan dengan tetap melakukan pengawasan dan pendampingan oleh pihak UIN Raden Fatah (PUSTIPD) saat pelaksanaan audit berlangsung.	Bersikap hati-hati terhadap persyaratan audit dan kegiatan yang melibatkan verifikasi sistem operasional.

9. C.13 Keamanan komunikasi

Tabel 3.9 Kondisi Implementasi Kontrol Keamanan Pada C.13

Klausul	**:**	**C.13 Keamanan komunikasi**
Kategori keamanan utama	**:**	**C.13.1 Manajemen keamanan jaringan** **C.13.2 Transfer Informasi**
Implementasi saat ini		**Implementasi ISO 27002:2013**
Kontrol keamanan C.13.1.1 Kontrol jaringan Sudah memiliki infranstruktur atau perangkat untuk melindungi sistem dan perangkat yang ada, dan pengendalian jaringan saat ini dipantau oleh unit PUSTIPD secara terus menerus. sehingga keamanan jaringan pada UIN Raden Fatah sudah dikelola secara baik dan benar.		Jaringan harus dikelola dan dikendalikan untuk melindungi informasi dalam sistem dan aplikasi.
Kontrol keamanan C.13.1.2 Keamanan layanan jaringan Saat ini mekanisme layanan jaringan disesuaikan dengan perkembangan kebutuhan yang diperlukan, dan tidak disertakan dalam perjanjian layanan jaringan.		Mekanisme keamanan, tingkat layanan, dan persyaratan manajemen dari semua layanan jaringan harus diidentifikasi dan disertakan dalam perjanjian layanan jaringan, apakah layanan ini disediakan secara internal atau *outsourcing*.
Kontrol keamanan C.13.1.3 Segeregasi dalam jaringan Terdapat pengelompokkan pengguna dalam akses sistem informasi.		Pada jaringan, bagi kelompok layanan informasi, pengguna dan sistem informasi harus dipisahkan.
Kontrol keamanan C.13.2.1 Kebijakan dan prosedur transfer informasi Saat ini belum terdapat kebijakan secara tertulis dalam prosedur transfer, sehingga kebijakan yang berjalan saat ini hanya berupa aturan atau perintah yang diberikan pimpinan PUSTIPD.		Kebijakan, prosedur, dan kontrol transfer formal harus ada untuk melindungi transfer informasi melalui penggunaan semua jenis fasilitas komunikasi.
Kontrol keamanan C.13.2.2 Perjanjian tentang transfer informasi Pengelolaan perjanjian tentang transfer informasi dikelola secara mandiri oleh organisasi masing-masing.		Perjanjian harus membahas transfer informasi bisnis yang aman.
Kontrol keamanan C.13.2.3 Pesan elektronik Saat ini sistem sudah menggunakan jalur https atau ssl.		Informasi yang terlibat dalam pesan elektronik harus dilindungi dengan tepat.
Kontrol keamanan C.13.2.4 Perjanjian kerahasian atau kerahasiaan Dalam pengelolaan identifikasi perjanjian kerahasiaan atau kerahasiaan dikelola oelh internal UIN Raden Fatah, melalui peninjauan yang dilakukan dalam bentuk monitoring atau evaluasi yang nantinya akan didokumentasi atau diarsipkan secara berkala oleh unit internal UIN Raden Fatah.		Persyaratan untuk perjanjian kerahasiaan atau non-pengungkapan yang mencerminkan kebutuhan organisasi untuk perlindungan informasi harus diidentifikasi, ditinjau dan didokumentasikan secara teratur.

10. C.14 Akusisi, pengembangan dan pemeliharaan sistem

Tabel 3.10 Kondisi Implementasi Kontrol Keamanan Pada C.14

Klausul	**:**	**C.14 Akusisi, pengembangan, dan pemeliharaan sistem**
Kategori keamanan utama	**:**	**C.14.1 Persyaratan keamanan sistem informasi** **C.14.2 Keamanan dalam proses pengembangan dan dukungan** **C.14.3 Data uji**
Implementasi saat ini		**Implementasi ISO 27002:2013**
Kontrol keamanan C.14.1.1 Analisis dan spesifikasi persyaratan keamanan informasi Dalam membuat suatu sistem informasi yang baru tetap menggunakan persyaratan keamanan informasi yang sudah ada, dan juga akan menambah persyaratan keamanan informasi hanya jika dibutuhkan saja dalam pembuatan maupun pengembangan sistem Informasi.		Persyaratan terkait keamanan informasi harus disertakan dalam persyaratan untuk new sistem informasi atau peningkatan sistem informasi yang ada.
Kontrol keamanan C.14.1.2 Mengamankan layanan aplikasi jaringan publik Upaya UIN Raden Fatah dalam melindungi aktivitas penipuan pada jaringan publik yaitu dengan menggunakan protokol "https". Sedangkan upaya UIN Raden Fatah dalam melindungi dari perselisihan kontrak dan pengungkapan serta perlindungan modifikasi yang tidak sah yaitu dengan membatasi hak akses masuk, melakukan pencatatan setiap perubahan data, dan melakukan pencadangan data.		Informasi yang terlibat dalam layanan aplikasi yang melewati jaringan publik harus dilindungi dari aktivitas penipuan, perselisihan kontrak dan pengungkapan serta modifikasi yang tidak sah.
Kontrol keamanan C.14.1.3 Melindungi transaksi layanan aplikasi Perlindungan transaksi layanan aplikasi pada UIN Raden Fatah sudah terlindungi dengan terhubungnya secara otomatis sistem pembayaran ukt antara pihak bank dan UIN Raden Fatah. Maka jika mahasiswa belum melakukan pembayaran dan ingin melakukan pembayaran, maka pihak bank akan menginput data pembayaran mahasiswa tersebut.		Informasi yang terlibat dalam transaksi layanan aplikasi harus dilindungi untuk mencegah ketidaklengkapan transmisi, mis-routing, perubahan pesan yang tidak sah, pengungkapan yang tidak sah, duplikasi atau replay pesan yang tidak sah.
Kontrol keamanan C.14.2.1 Kebijakan pembangunan yang aman Sudah terdapat Standard Operating Procedure (SOP) pengembangan aplikasi dan website. Namun pada pelaksanaannya pengembangan perangkat lunak dan sistem pada UIN Raden Fatah yang dikelola oleh divisi developer dilakukan secara flexible mengikuti kebutuhan yang diinginkan. Dalam pengembangan sistem informasi pada UIN Raden Fatah juga tidak mengikuti SOP yang sudah dibuat, seperti dalam pembuatan, pengembangan, dan		Aturan untuk pengembangan perangkat lunak dan sistem harus ditetapkan dan diterapkan pada pengembangan dalam organisasi.

pemeliharaan sistem informasi tersebut dilakukan oleh satu orang yang sama dengan mengendalikan keahliannya.	

Tabel 3.10 Kondisi Implementasi Kontrol Keamanan Pada C.14 Lanjutan

Klausul	**:**	**C.14 Akusisi, pengembangan, dan pemeliharaan sistem**
Kategori keamanan utama	**:**	**C.14.1 Persyaratan keamanan sistem informasi** **C.14.2 Keamanan dalam proses pengembangan dan dukungan** **C.14.3 Data uji**

Implementasi saat ini	Implementasi ISO 27002:2013
Kontrol keamanan C.14.2.2 Prosedur pengendalian perubahan sistem Pada UIN Raden Fatah prosedur pengendalian perubahan sistem dilakukan secara flexibel sesuai dengan kebutuhan dan dilakukan berdasarkan prosedur yang diketahui developer.	Perubahan sistem dalam siklus hidup pengembangan harus dikendalikan dengan menggunakan perubahan prosedur pengendalian formal.
Kontrol keamanan C.14.2.3 Tinjauan teknis aplikasi setelah perubahan platform operasi Peninjauan *platform* operasi dilakukan kembali jika terdapat perubahan dengan menyediakan SOP dan pedoman (tata cara) dalam mengoperasikan aplikasi. UIN Raden Fatah juga melakukan pengujian kembali terhadap perubahan *platform* operasi yang terjadi, dengan melakukan uji t*esting* sebelum disebarkan kepada pengguna.	Ketika platform operasi diubah, aplikasi penting bisnis harus ditinjau dan diuji untuk memastikan tidak ada dampak buruk pada operasi atau keamanan organisasi.
Kontrol keamanan C.14.2.4 Pembatasan perubahan pada paket perangkat lunak Saat ini UIN Raden Fatah menerapkan pembatasan modifikasi pada paket perangkat lunak yang ada, sehinggan modifikasi akan dilakukan berdasarkan analisis kebutuhan yang diinginkan, maka jika terdapat penambahan kebutuhan yang diperlukan oleh UIN Raden Fatah, maka akan ditambahkan, dan sebaliknya.	Modifikasi paket perangkat lunak tidak boleh dilakukan, terbatas pada perubahan yang diperlukan dan semua perubahan harus dikontrol secara ketat.
Kontrol keamanan C.14.2.5 Prinsip-prinsip rekayasa sistem yang aman Sudah memiliki SOP dalam pengembangan sistem informasi, dimana seharusnya dalam pengembangan sistem informasi *developer* akan membuat sebuah modul yang yang mebahas mengenai *requirement planning* sistem informasi yang ingin dikembangkan/dibuat. Namun pada praktiknya saat ini belum berjalan/dilakukan. Saat ini Implementasi prinsip-prinsip rekayasa sistem tersebut diterapkan dengan menyesuaikan sistem informasi yang dibutuhkan. Prinsip tersebut tidak tertulis, dan dilakukan berdasarkan kebutuhan dan kopetensi yang dimiliki oleh *developer* sistem .	Prinsip-prinsip untuk sistem keamanan rekayasa harus ditetapkan, didokumentasikan, dipelihara, dan diterapkan untuk setiap upaya implementasi sistem informasi.

Tabel 3.10 Kondisi Implementasi Kontrol Keamanan Pada C.14 Lanjutan

Klausul	**:**	**C.14 Akusisi, pengembangan, dan pemeliharaan sistem**
Kategori keamanan utama	**:**	**C.14.1 Persyaratan keamanan sistem informasi** **C.14.2 Keamanan dalam proses pengembangan dan dukungan** **C.14.3 Data uji**

Implementasi saat ini	Implementasi ISO 27002:2013
Kontrol keamanan C.14.2.6 Lingkungan pengembangan yang aman Saat ini UIN Raden Fatah sudah memiliki lingkungan pengembangan sistem yang aman baik dari proses, teknologi, serta fasilitas keamanan lingkungan yang mendukung.	Organisasi harus menetapkan dan secara tepat melindungi lingkungan pengembangan yang aman untuk sistem upaya pengembangan dan integrasi yang mencakup seluruh siklus hidup pengembangan sistem.
Kontrol keamanan C.14.2.7 Pengembangan yang dialihdayakan Pengawasan dan pemantauan pengembangan sistem yang dialihdayakan dikelola langsung oleh developer pertama yang mengembangkan/membuat sistem tersebut.	Organisasi harus mengawasi dan memantau aktivitas pengembangan sistem yang dialihdayakan.
Kontrol keamanan C.14.2.8 Pengujian keamanan sistem Pengujian keamanan sistem pada pengujian fungsional dari sistem yang sudah dibuat akan dilakukan pengujian, sampai sistem tersebut dinyatakan tidak terdapat *error*. Jika pada saat pengujian terdapat kendala *(error)*, maka akan diperbaiki, sedangkan jika saat pengujian tidak terdapat kendala *(unerror),* maka tidak akan ada pengujian kembali, sampai nanti dibutuhkan waktu pengujian kembali.	Pengujian fungsionalitas keamanan harus dilakukan selama pengembangan.
Kontrol keamanan C.14.2.9 Pengujian penerimaan sistem Saat ini UIN Raden Fatah (PUSTIPD) hanya melakukan pengujian data secara fungsional saja dalam lingkup internal, dan belum melakukan jenis pengujian sistem lainnya.	Program pengujian penerimaan dan kriteria terkait harus ditetapkan untuk sistem informasi baru, upgrade dan versi baru.
Kontrol keamanan C.14.3.1 Perlindungan data uji Pengendalian data uji pada UIN Raden Fatah saat ini belum dilakukan secara maksimal. Karena uji data yang dilakukan hanya uji data fungsional dalam lingkup internal. Pemilihan data uji yang akan digunakan dalam proses uji coba dipilih berdasarkan kerahasiaan data yang digunakan. Data uji yang telah digunakan, setelahnya akan dihapus dalam riwayat *database* pada sistem.	Data uji harus dipilih dengan hati-hati, dilindungi dan dikendalikan.

11. C.15 Hubungan pemasok

Tabel 3.11 Kondisi Implementasi Kontrol Keamanan Pada C.15

Klausul	**:**	**C.15 Hubungan pemasok**
Kategori keamanan utama	**:**	**C.15.1 Keamanan informasi dalam hubungan pemasok** **C.15.2 Manajemen pengiriman layanan produk**
Implementasi saat ini		**Implementasi ISO 27002:2013**
Kontrol keamanan C.15.1.1 Kebijakan keamanan informasi untuk hubungan pemasok Kebijakan keamanan informasi hubungan pemasok pada UIN Raden Fatah secara khusus belum dimiliki, tetapi saat ini kebijakan ini didokumentasikan dalam bentuk persetujuan persyaratan berupa surat perjanjian kontrak antara UIN Raden Fatah dan mitra yang bekerjasama.		Persyaratan keamanan informasi untuk mengurangi risiko yang terkait dengan akses pemasok ke aset organisasi harus disetujui dengan pemasok dan didokumentasikan.
Kontrol keamanan C.15.1.2 Mengatasi keamanan dalam perjanjian pemasok Dalam mengatasi keamanan dalam perjanjian pemasok, UIN Raden Fatah menetapkan persyaratan keamanan informasi berdasarkan keputusan dan kesepakatan bersama antara pemasok dan UIN Raden Fatah yang didokumentasikan dalam bentuk surat perjanjian kontrak.		Semua persyaratan keamanan informasi yang relevan harus ditetapkan dan disepakati dengan masing-masing pemasok yang dapat mengakses, memproses, menyimpan, mengomunikasikan, atau menyediakan komponen infrastruktur TI untuk, informasi organisasi.
Kontrol keamanan C.15.1.3 Rantai pasokan teknologi informasi dan komunikasi Penerapan yang dilakukan dalam kesesuaian rantai pemasok dengan persyaratan keamanan informasi dilakukan berdasarkan keputusan dan kesepakatan bersama antara pemasok dan UIN Raden Fatah yang didokumentasikan dalam bentuk surat perjanjian kontrak.		Perjanjian dengan pemasok harus mencakup persyaratan untuk mengatasi risiko keamanan informasi terkait dengan layanan teknologi informasi dan komunikasi dan rantai pasokan produk.
Kontrol keamanan C.15.2.1 Pemantauan dan peninjauan layanan pemasok Dalam menerima layanan pemasok, tidak dilakukan pemantauan secara berkala (audit). Tetapi pemantauan dan peninjauan dilakukan sekali pada saat uji testing layanan, jika tidak terdapat kendala, maka tidak dilakukan pemantauan kembali, sesuai dengan masa garansi.		Organisasi harus secara teratur memantau, meninjau, dan mengaudit pemberian layanan pemasok.
Kontrol keamanan C.15.2.2 Mengelola perubahan pada layanan pemasok Saat ini perubahan penyediaan layanan pemasok dilakukan jika layanan tersebut tidak cocok untuk dipakai.		Perubahan pada penyediaan layanan oleh pemasok, termasuk mempertahankan dan meningkatkan yang sudah ada kebijakan, prosedur, dan kontrol keamanan informasi, harus dikelola, dengan mempertimbangkan: kekritisan informasi bisnis, sistem dan proses yang terlibat dan penilaian ulang risiko.

12. C.16 Manajemen insiden keamanan informasi

Tabel 3.12 Kondisi Implementasi Kontrol Keamanan Pada C.16

Klausul	**:**	**C.16 Manajemen insisden keamanan informasi**
Kategori keamanan utama	**:**	**C.16.1 Manajemen insiden dan peningkatan keamanan informasi**

Implementasi saat ini	**Implementasi ISO 27002:2013**
Kontrol keamanan C.16.1.1 Tanggung jawab dan prosedur Tanggung jawab manajemen keamanan sistem informasi pada UIN Raden Fatah sudah ditetapkan dan di sepakati oleh setiap pihak (pengelola) terkait dalam bentuk Surat Perjanjian Kerja dan SK. Sedangkan prosedur manajemen keamanan sistem infromasi pada UIN Raden Fatah sudah ditetapkan dan dilampirkan dalam bentuk SOP *(Standard Operating Procedure)*, tetapi masih secara umum.	Tanggung jawab dan prosedur manajemen harus ditetapkan untuk memastikan proses yang cepat, efektif dan respon tertib terhadap insiden keamanan informasi.
Kontrol keamanan C.16.1.2 Melaporkan peristiwa keamanan informasi Pelaporan peristiwa keamanan informasi pada UIN Raden Fatah dapat melalui telepon (0711354668), email pustipd_uin@radenfatah.ac.id atau melalui website https://help.radenfatah.ac.id	Peristiwa keamanan informasi harus dilaporkan melalui saluran manajemen yang sesuai sebagai: secepat mungkin.
Kontrol keamanan C.16.1.3 Melaporkan kelemahan keamanan informasi Pencatatan kelemahan keamanan pada sistem informasi dapat dilakukan dengan mengirimkan informasi tersebut kepada unit PUSTIPD melalui telepon (0711354668), email pustipd_uin@radenfatah.ac.id atau melalui website https://help.radenfatah.ac.id	Karyawan dan kontraktor yang menggunakan sistem dan layanan informasi organisasi harus diminta untuk mencatat dan melaporkan setiap kelemahan keamanan informasi yang diamati atau dicurigai dalam sistem atau layanan.
Kontrol keamanan C.16.1.4 Penilaian dan keputusan tentang peristiwa keamanan informasi Saat ini UIN Raden Fatah diwakilkan oleh unit PUSTIPD dalam melakukan penilaian terkait peristiwa keamanan informasi yang berpotensi mengancam keamanan informasi dengan memberikan laporan dari hasil evaluasi yang telah dilakukan.	Peristiwa keamanan informasi harus dinilai dan harus diputuskan apakah akan diklasifikasikan sebagai: insiden keamanan informasi.
Kontrol keamanan C.16.1.5 Tanggapan terhadap insisden keamanan informasi Setiap insisden keamanan informasi pada UIN Raden Fatah akan ditanggapi melalui unit PUSTIPD melalui laporan yang sudah disampaikan dengan mengikuti prosedur sesuai dengan SOP yang dapat dilihat pada website pustipd.radenfatah.ac.id	Insiden keamanan informasi harus ditanggapi sesuai dengan prosedur terdokumentasi.

Tabel 3.12 Kondisi Implementasi Kontrol Keamanan Pada C.16 Lanjutan

Klausul	**:**	**C.16 Manajemen insisden keamanan informasi**
Kategori keamanan utama	**:**	**C.16.1 Manajemen insiden dan peningkatan keamanan informasi**
Implementasi saat ini		**Implementasi ISO 27002:2013**
Kontrol keamanan C.16.1.6 Belajar dari insiden keamanan informasi UIN Raden Fatah selalu mengevaluasi setiap insiden keamanan informasi yang pernah terjadi sebelumnya.		Pengetahuan yang diperoleh dari menganalisis dan menyelesaikan insiden keamanan informasi harus digunakan untuk mengurangi kemungkinan atau dampak insiden di masa depan.
Kontrol keamanan C.16.1.7 Pengumpulan bukti Prosedur pelaporan dapat dilakukan dengan membuat laporan yang disertai dengan bukti terlampir seperti foto atau laporan layanan dari pengguna. Kendala IT yang terjadi akan di dokumentasikan sebagai bukti saat pelaporan kepada pihak manajemen terkait penyedia aset pada UIN Raden Fatah.		Organisasi harus menetapkan dan menerapkan prosedur untuk identifikasi, pengumpulan, perolehan dan pelestarian informasi, yang dapat berfungsi sebagai bukti.

C.17 Aspek keamanan informasi dari manajemen kelangsungan bisnis

Tabel 3.13 Kondisi Implementasi Kontrol Keamanan Pada C.17

Klausul	**:**	**C.17 Aspek keamanan informasi dari manajemen kelangsungan bisnis**
Kategori keamanan utama	**:**	**C.17.1 Kesinambungan keamanan informasi** **C.17.2 Redundansi**
Implementasi saat ini		**Implementasi ISO 27002:2013**
Kontrol keamanan C.17.1.1 Merencanakan kesinambungan keamanan informasi a. Sistem informasi pada UIN Raden Fatah sudah memiliki teknologi HA *(High Available)*. b. Perangkat pengolahan informasi sudah memiliki sistem yang redudan *(mirroring)*, dimana terdapat 2 perangkat yang sama yang saling membackup (mencadangkan) ketika terjadi masalah.		Organisasi harus menentukan persyaratannya untuk keamanan informasi dan kelangsungan manajemen keamanan informasi dalam situasi yang merugikan, misalnya selama krisis atau bencana.
Kontrol keamanan C.17.1.2 Menerapkan kontinuitas keamanan informasi a. Sudah menerapkan prosedur teknologi HA *(High Available)* dengan menyediakan dan menggunakan perangkat sistem yang redudan *(mirroring)*, dimana terdapat 2 perangkat yang sama yang saling *backup* (mencadangkan) ketika terjadi masalah secara otomatis.		Organisasi harus menetapkan, mendokumentasikan, menerapkan dan memelihara proses, prosedur dan kontrol

Tabel 3.13 Kondisi Implementasi Kontrol Keamanan Pada C.17 Lanjutan

Klausul	**:**	**C.17 Aspek keamanan informasi dari manajemen kelangsungan bisnis**
Kategori keamanan utama	**:**	**C.17.1 Kesinambungan keamanan informasi** **C.17.2 Redundansi**
Implementasi saat ini		**Implementasi ISO 27002:2013**
b. Dokumentasi yang dilakukan berupa dokumen *logic* sistem berbentuk diagram keberlangsungan sistem. c. Pemeliharaan proses yang dilakukan dengan memperpanjang proses masa garansi dari pengadaan perangkat. d. Pemeliharaan proses yang dilakukan dengan memperpanjang proses masa garansi dari pengadaan perangkat. Sedangkan pemeliharaan prosedur dilakukan dengan kegiatan monitoring untuk memastikan teknologi HA yang digunakan tetap dalam keadaan layak untuk digunakan. e. Sudah terdapat *form* kontrol audit IT yang disimpan oleh unit PUSTIPD, namun dalam penerapannya belum dilakukan.		untuk memastikan tingkat kesinambungan yang diperlukan untuk keamanan informasi selama situasi yang merugikan.
Kontrol keamanan C.17.1.3 Memverifikasi, meninjau, dan mengevaluasi kesinambungan keamanan informasi Saait ini verifikasi kesinambungan keamanan dikelola oleh unit PUSTIPD dengan melakukan pengecekan *dashboard* pengolahan informasi yang disajikan dalam bentuk grafik yang terdapat pada ruang *server* dan *center* PUSTIPD.		Organisasi harus memverifikasi kesinambungan keamanan informasi yang ditetapkan dan diterapkan kontrol secara berkala untuk memastikan bahwa mereka valid dan efektif selama situasi yang merugikan.
Kontrol keamanan C.17.2.1 Ketersediaan fasilitas pepmprosesan informasi Fasilitas pemprosesan informasi pada UIN Raden Fatah sudah menginplementasikan redudansi pada perangkat dan kelistrikan.		Fasilitas pemrosesan informasi harus diimplementasikan dengan redundansi yang cukup untuk memenuhi ketersediaan persyaratan.

13. C.18 Kepatuhan

Tabel 3.14 Kondisi Implementasi Kontrol Keamanan Pada C.18

Klausul	**:**	**C.18 Kepatuhan**
Kategori keamanan utama	**:**	**C.18.1 Kepatuhan terhadap persyaratan hukum dan kontrak** **C.18.2 Tinjauan keamanan informasi**
Implementasi saat ini		**Implementasi ISO 27002:2013**
Kontrol keamanan C.18.1.1 Identifikasi peraturan perundang-undangan dan persyaratan yang berlaku Saat ini sistem keamanan UIN Raden Fatah sudah mematuhi peraturan-peraturan yang berlaku, baik dalam pengendalian akses dan pemakaian sistem yang digunakan sesuai dengan		Semua undang-undang legislatif yang relevan, peraturan, persyaratan kontrak dan pendekatan organisasi untuk memenuhi persyaratan ini harus secara eksplisit diidentifikasi, didokumentasikan dan terus diperbarui untuk setiap sistem informasi dan organisasi.

kebutuhan pendidikan. Pendokumentasian yang dilakukan disesuaikan dengan jenis kebutuhan yang ada, seperti surat perjanjian, kontrak kerja, SK, dan SOP. Sedangkan dalam pembaruan kebijakan tidak dilakukan secara berkala, sehingga pembaruan akan menyesuaikan himbaun pimpinan internal UIN Raden Fatah maupun pimpinan PUSTIPD dengan memperhatikan kebutuhan kondisi saat itu.\	
Kontrol keamanan C.18.1.2 Hak kekayaan intelektual Setiap produk perangkat lunak yang dimiliki oleh UIN Raden Fatah sebagai aset pengolaan informasi didapatkan secara legal dari pemerintah dan donatur yang diproses dengan prosedur yang tidak menentang undang-undang dan sesuai dengan peraturan yang berlaku serta mengikuti persyaratan kontrak (kerjasama) yang sudah disepakati bersama.	Prosedur yang tepat harus diterapkan untuk memastikan kepatuhan dengan undang-undang, peraturan dan persyaratan kontrak yang terkait dengan hak kekayaan intelektual dan penggunaan produk perangkat lunak berpemilik.
Kontrol keamanan C.18.1.3 Perlindangan catatan Saat ini upaya dalam perlindungan data informasi yaitu menerapkan SOP dalam pembatasan dan pengawasan akses masuk baik dalam sistem maupun area ingkungan pengolahan data, dan menyediakan penanggung jawab dalam perlindungan data informasi. Tetapi saat ini kebijakan perlindungan data informasi pada UIN Raden Fatah belum memiliki persyaratan bisnis secara khusus, sehingga menyesuaikan dengan keputusan bersama dan kebutuhan saat itu.	Catatan harus dilindungi dari kehilangan, kehancuran, pemalsuan, akses tidak sah dan tidak sah rilis, sesuai dengan peraturan perundang-undangan, peraturan, kontrak dan persyaratan bisnis.
Kontrol keamanan C.18.1.4 Privasi dan perlindungan informasi pengenal pribadi Saat ini privasi dan perlindungan informasi yang ada dapat dipertanggungjawabkan kejaminan kerahasiaannya, karena setiap akses memiliki perizinannya masing-masing yang disesuaikan dengan tipe pengguna. Selain itu penerapan manajemen keamanan informasi pada lingkungan UIN Raden Fatah juga mendukung perlindungan privasi dan data informasi, karena dilengkapi dengan kebijakan SOP, fasilitas keamanan dan penggunaan enkripsi.	Privasi dan perlindungan informasi yang dapat diidentifikasi secara pribadi harus dipastikan seperti yang dipersyaratkan dalam relevan perundang-undangan dan peraturan yang berlaku.

Tabel 3.14 Kondisi Implementasi Kontrol Keamanan Pada C.18 Lanjutan

Klausul	**:**	**C.18 Kepatuhan**
Kategori keamanan utama	**:**	**C.18.1 Kepatuhan terhadap persyaratan hukum dan kontrak** **C.18.2 Tinjauan keamanan informasi**
Implementasi saat ini		**Implementasi ISO 27002:2013**
Kontrol keamanan C.18.1.5 Regulasi kontrol kadafi Saat ini kebijakan kontrol kriptografi belum dikelola dan didokumentasikan secara khusus. Sehingga kontrol kriptografi dalam pelaksanaan teknis penggunaan enkripsi dilakukan berdasarkan kesepakatan bersama pihak PUSTIPD, dan menyesuaikan kebutuhan sistem informasi dengan mengikuti prosedur enkripsi yang sesuai pemahaman penggunaan dan peraturan enkripsi yang digunakan pada sistem dengan tetap mematuhi peraturan undang-undang.		Kontrol kriptografi harus digunakan sesuai dengan semua perjanjian, undang-undang dan peraturan.
Kontrol keamanan C.18.2.1 Tinjauan independent terhadap keamanan informasi Saat ini tinjauan indipenden terhadap keamanan baik dalam peninjauan pengendalian tujuan keamanan informasi, kontrol keamanan informasi, kebijakan keamanan informasi, proses keamanan informasi, dan prosedur keamanan informasi sudah dilakukan secara 32ndependent, tetapi belum pada interval yang direncanakan (secara berkala).		Pendekatan organisasi untuk mengelola keamanan informasi dan implementasinya (yaitu pengendalian tujuan, kontrol, kebijakan, proses dan prosedur untuk keamanan informasi) harus ditinjau independen pada interval yang direncanakan atau ketika perubahan signifikan terjadi.
Kontrol keamanan C.18.2.2 Kepatuhan terhadap kebijakan dan standar keamanan Saat ini peninjauan kepatuhan terhadap kebijakan dan standar keamanan sistem informasi belum dilakukan secara berkala, namun dilakukan jika diperlukan saja *(by accident)* yang disesuaikan dengan situasi yang terjadi.		Manajer harus secara teratur meninjau kepatuhan pemrosesan informasi dan prosedur dalam wilayah tanggung jawab mereka dengan kebijakan keamanan yang sesuai, standar dan keamanan lainnya persyaratan.
Kontrol keamanan C.18.2.3 Tinjauan kepatuhan teknis Saat ini tinjauan terhadap kepatuhan teknis baik dalam kebijakan dan standar keamanan sistem informasi belum dilakukan secara berkala, namun dilakukan jika diperlukan saja *(by accident)* yang disesuaikan dengan situasi yang terjadi.		Sistem informasi harus ditinjau secara teratur untuk kepatuhan dengan informasi organisasi kebijakan dan standar keamanan.

Berikut ini rekapitulasi hasil perhitungan *Maturity Level* Klausul ISO/IEC 27002:2013 pada UIN Raden Fatah yang dapat dilihat pada tabel 3.15 yaitu:

Tabel 3.15 Rekapitulasi Hasil Penilaian *Capability Level* dan *Maturity Level* Klausul ISO/IEC 27002:2013 Pada UIN Raden Fatah

Klausul	Nama Klausul	Hasil Nilai CL	Tingkat Capability Level	Hasil Nilai ML	Tingkat Maturity Level	Keterangan CL/ML
C.5	Kebijkan Keamanan Informasi	2	2	2	2	*Managed*
C.6	Organisasi Keamanan Informasi	1,8	2	1,9	2	*Managed*
C.7	Keamanan Sumber Daya Manusia	2,16	2	2,30	2	*Managed*
C.8	Manajemen Aset	2,3	3	2,3	2	*Defined/ Managed*
C.9	Kontrol Akses	2,05	2	2,4	2	*Managed*
C.10	Kriptografi	0	0	1	1	*Incomplete /Initial*
C.11	Keamanan Fisik dan Lingkungan	2,40	3	3,35	3	*Defined*
C.12	Operasi Keamanan	2,07	2	2,41	2	*Managed*
C.13	Keamanan Komunikasi	2	2	2	2	*Managed*
C.14	Akusisi, pengembangan dan pemeliharaan sistem	1,92	2	2,16	2	*Managed*
C.15	Hubungan pemasok	1,80	2	1,9	2	*Managed*
C.16	Manajemen insiden keamanan informasi	2,21	2	2,64	3	*Managed/ Defined*
C.17	Aspek keamanan informasi dari manajemen kelangsungan bisnis	2,75	3	4,38	5	*Defined/ Optimizing*
C.18	Kepatuhan	1,93	2	2,03	2	*Managed*
Rata-rata		**1,96**	**2**	**2,34**	**2**	***Managed***

Maka dari hasil penilaian di atas maka dapat disimpulkan bahwa besar nilai keamanan sistem informasi pada UIN Raden Fatah Palembang menggunakan standar ISO/IEC 27002:2013 untuk nilai *capability level* yaitu sebesar 1,96 sedangkan untuk nilai *maturity level* yaitu sebesar 2,34 dan sama-sama berada pada level 2 *(Managed)*.

BAB IV
REKOMENDASI

Berikut adalah rekomendasi terhadap temuan evaluasi tata kelola keamanan sistem informasi menggunakan ISO/IEC 27002:2013 pada UIN Raden Fatah yaitu:

1. C.5 Kebijakan keamanan informasi

Tabel 4.1 Rekomendasi Kontrol Keamanan Pada C.5

Kontrol Keamanan	Rekomendasi
C.5.1.1 Kebijakan untuk keamanan informasi	Membuat serangkaian kebijakan untuk keamanan informasi secara lengkap dan diterbitkan dalam bentuk dokumen tertulis yang ditetapkan dan disetujui sesuai dengan peraturan keamanan sistem informasi dan peraturan yang signifikan Adapun panduan implementasi yang dapat dilakukan yaitu: a. Pada tingkat tertinggi, organisasi harus menetapkan "kebijakan keamanan informasi" yang disetujui oleh manajemen dan yang menetapkan pendekatan organisasi untuk mengelola tujuan keamanan informasinya. Sedangkan pada tingkatan yang lebih rendah, kebijakan keamanan informasi harus didukung oleh kebijakan khusus topik, yang lebih lanjut mengamanatkan pelaksanaan kontrol keamanan informasi dan biasanya terstruktur untuk mengatasi kebutuhan kelompok sasaran tertentu dalam suatu organisasi atau untuk menutupi topik tertentu. b. Kebijakan keamanan informasi harus memenuhi persyaratan yang dibuat oleh strategi bisnis, peraturan, perundang-undangan, dan kontrak, serta lingkungan ancaman keamanan informasi saat ini dan yang diproyeksikan. c. Kebijakan keamanan informasi harus berisi pernyataan tentang: - Definisi keamanan informasi, tujuan dan prinsip untuk memandu semua kegiatan yang berkaitan dengan informasi keamanan. - Penugasan tanggung jawab umum dan khusus untuk manajemen keamanan informasi untuk peran yang ditentukan. - Proses penanganan penyimpangan dan pengecualian. d. Contoh topik kebijakan keamanan informasi tersebut berupa kontrol akses, klasifikasi informasi (dan penanganannya), keamanan fisik dan lingkungan, topik berorientasi pengguna akhir (penggunaan aset yang dapat diterima, *clear desk* dan *clear screen*, transfer informasi, perangkat seluler dan kerja jarak jauh, pembatasan instalasi dan penggunaan perangkat lunak), cadangan, transfer informasi, perlindungan dari malware, pengelolaan kerentanan teknis, kontrol kriptografi, keamanan komunikasi, privasi dan perlindungan informasi yang dapat didefinisikan secara pribadi, dan hubungan pemasok. e. Kebijakan ini harus dikomunikasikan kepada karyawan dan pihak eksternal terkait dalam bentuk yang signifikan dapat diakses, dan dapat dipahami oleh pembaca yang dituju, misalnya dalam konteks "informasi" kesadaran keamanan, program pendidikan dan pelatihan"
C.5.1.2 Tinjauan kebijakan untuk keamanan informasi	Kebijakan untuk keamanan informasi harus ditinjau pada interval yang direncanakan agar dapat memastikan kesesuaian, kecukupan, dan keefektifannya yang berkelanjutan. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Setiap kebijakan harus memiliki pemilik yang telah menyetujui tanggung jawab manajemen untuk pengembangan, review dan evaluasi kebijakan. b. Tinjauan harus mencakup penilaian peluang untuk perbaikan kebijakan dan pendekatan organisasi untuk mengelola keamanan informasi dalam menanggapi perubahan terhadap lingkungan organisasi, keadaan bisnis, kondisi hukum atau lingkungan teknis.

Tabel 4.1 Rekomendasi Kontrol Keamanan Pada C.5 Lanjutan

Kontrol Keamanan	Rekomendasi
	c. Tinjauan kebijakan untuk keamanan informasi harus mempertimbangkan hasil tinjauan manajemen. d. Memperoleh persetujuan manajemen untuk kebijakan yang akan direvisi.

2. C.6 Organisasi keamanan informasi

Tabel 4.2 Rekomendasi Kontrol Keamanan Pada C.6

Kontrol Keamanan	Rekomendasi
C.6.1.1 Peran dan tanggung jawab keamanan informasi	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat peran dan penanggungjawab keamanan sistem informasi pada organisasi.
C.6.1.2 Pemisahan tugas	Tugas dan area tanggung jawab yang saling bertentangan harus dipisahkan untuk mengurangi peluang bagi modifikasi yang tidak sah atau tidak disengaja atau penyalahgunaan aset organisasi. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Organisasi harus memperhatikan bahwa tidak ada satu orang pun yang dapat mengakses, mengubah atau menggunakan aset tanpa izin atau deteksi. b. Inisiasi suatu peristiwa harus dipisahkan dari otoritasinya, karena kemungkinan dalam merangcang kontrol, kolusi harus dipertimbangkan kembali. c. Organisasi kecil mungkin sulit dalam melakukan pemisahan tugas, namun tetap harus diterapkan dan dilaksanakan sebisa mungkin.
C.6.1.3 Kontak dengan pihak berwewenang	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat pihak yang berwewenang menanggapi insiden keamanan sistem informasi pada organisasi.
C.6.1.4 Kontak dengan kelompok minat khusus	Organisasi harus memiliki kontak dengan forum keamanan khusus dan professional. Adapun panduan implementasi yang dapat dilakukan yaitu dengan mencari kelompok atau forum keamanan khusus yang dapat dipastikan mampu dalam: a. Meningkatkan pengetahuan tentang praktik terbaik dan tetap *up to date* dengan informasi keamanan yang signifikan b. Memastikan pemahaman tentang lingkungan keamanan informasi terrkini dan lengkap. c. Menerima peringatan dini yang berkaitan dengan serangan dari kerentanan. d. Memiliki akses ke spesialis keamanan informasi. e. Berbagi dan bertukar informasi tentang teknologi, produk, ancaman, atau kerentanan baru. f. Memberikan titik penghubung yang sesuai ketika menangani insiden keamanan informasi.
C.6.1.5 Keamanan informasi dalam manajemen proyek	Keamanan informasi harus ditangani dalam manajemen proyek, terlepas dari jenis proyeknya, Adapun panduan implementasi yang dapat dilakukan yaitu: a. Keamanan informasi harus diintegrasikan ke dalam metode manajemen proyek organisasi untuk memastikan bahwa resiko keamanan informasi diidentifikasi dan ditangani sebagai bagian dari proyek.

Tabel 4.2 Rekomendasi Kontrol Keamanan Pada C.6 Lanjutan

Kontrol Keamanan	Rekomendasi
C.6.2.1 Kebijakan perangkat seluler	Kebijakan dan langkah-langkah keamanan pendukung harus dimiliki untuk mengelola resiko yang diperkenalkan dengan menggunakan perangkat seluler. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Saat menggunakan perangkat seluler, perhatian khusus harus diberikan untuk memastikan bahwa informasi bisnis tidak dikompromikan. Kebijakan perangkat seluler harus mempertimbangkan resiko bekerja dengan perangkat yang tidak terlindungi. Adapun hal yang perlu dipertimbangkan yaitu, pendaftaran perangkat seluler, persyaratan untuk perlindungan fisik, pembatasan instalasi perangkat lunak, pembatasan koneksi ke layanan informasi, kontrol akses, perlindungan malware, cadangan, dan penggunaan layanan aplikasi. b. Perangkat seluler harus dilindungi secara fisik dari ancaman di lingkungan tempat umum. c. Jika kebijakan perangkat seluler mengizinkan penggunaan perangkat seluler pribadi, maka hal yang perlu dipertimbangkan yaitu: - Pemisahan penggunaan perangkat untuk keperluan pribadi dan bisnis. - Menyediakan akses ke informasi bisnis hanya setelah pengguna menandatangani perjanjian pengguna akhir mengakui tugas mereka. - Melepaskan kepemilikan atas data bisnis, memungkinkan penghapusan data jarak jauh oleh organisasi jika terjadi pencurian atau kehilangan perangkat ketika tidak lagi berwewnang untuk menggunakan layanan.
C.6.2.2 Kerja jarak jauh	Organisasi harus menerapkan dan mengeluarkan kebijakan dan langkahlangkah keamanan yang menggambarkan kondisi dan pembatasan dalam penggunaan kerja jarak jauh. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Mengeluarkan kebijakan yang memuat tentang aturan kerja jarak jauh yang memperhatikan hal-hal berikut: - Keamanan fisik (bangunan & lingkungan) yang terdapat di lokasi jarak jauh. - Lingkungan kerja jarak jauh yang diusulkan. - Peraturan atau persyaratan keamanan komunikasi. - Penyediaan akses *desktop* virtual dan pencegahan ancaman akses yang tidak sah ke informasi atau sumber daya dari orang lain yang menggunakan akomodasi, seperti keluarga dan teman. - Penggunaan jaringan rumah dan persyaratan atau pembatasan konfigurasi nirkabel layanan jaringan. - Peraturan akses ke peralatan milik pribadi dan perlindungan *malware* dan persyaratan *firewall.*

1. C.7 Keamanan sumber daya manusia

Tabel 4.3 Rekomendasi Kontrol Keamanan Pada C.7

Kontrol Keamanan	Rekomendasi
C.7.1.1 Penyaringan	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat peraturan, hukum, dan etika yang relevan dalam proses penyaringan kandidat pegawai pada organisasi.
C.7.1.2 Syarat dan ketentuan kerja	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat perjanjian kontrak berupa pernyataan bahwa pegawai siap untuk bertanggung jawab terhadap tugas yang diberikan oleh organisasi.

Tabel 4.3 Rekomendasi Kontrol Keamanan Pada C.7 Lanjutan

Kontrol Keamanan	Rekomendasi
C.7.2.1 Tanggung jawab manajemen	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan keamanan sistem pada organisasi.
C.7.2.2 Kesadarn, pendidikan dan pelatihan keamanan informasi	Semua pegawai organisasi maupun pihak ketiga harus mendapatkan kesadaran pendidikan pelatihan, dan pembaruan secara rutin kebijakan dan prosedur organisasi yang signifikan dengan tugas pekerjaannya. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Program kesadaran keamanan informasi harus bertujuan untuk membuat pegawai dan pihak ketiga menyadari tanggung jawab mereka dalam hal keamanan informasi. b. Program kesadaran keamanan informasi harus ditetapkan sejalan dengan kebijakan keamanan informasi yang dimiliki. Seperti membuat program hari keamanan informasi dan menerbitkan buletin. c. Program penyadaran harus direnakan dengan mempertimbangkan peran pegawai dalam organisasi. d. Pelatihan kesadaran harus dilakukan seperti membuat pelatihan pembelajaran baik kelas jarak jauh, berbasis web, maupun mandiri. e. Pendidikan dan pelatihan keamanan harus dilakukan secara berkala. Program ini harus dijadwalkan dari waktu ke waktu secara teratur, sehingga tetap sejalan dengan kebijakan dan prosedur organisasi, dan dapat juga bermanfaat bagi pegawai baru.
C.7.2.3 Proses pendisiplinan	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat proses disipliner formal yang dikomunikasikan kepada pegawai mengenai pengambilan tindakan terhadap pegawai yang melakukan pelanggaran keamanan informasi pada organisasi.
C.7.3.1 Pemutusan atau perubahan tanggung jawab pekerjaan	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan kebijakan mengenai pemutusan atau perubahan tanggung jawab pekerjaan pada pegawai organisasi.

2. C.8 Manajemen aset

Tabel 4.4 Rekomendasi Kontrol Keamanan Pada C.8

Kontrol Keamanan	Rekomendasi
C.8.1.1 Invetarisasi aset	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat proses inventarisasi aset, yang meliputi pendataan, pemprosesan, penyimpanan,dan pemeliharaan aset.
C.8.1.2 Kepemilikan aset	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penanggungjawab dari masing-masing aset organisasi.
C.8.1.3 Penggunaan aset yang dapat diterima	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah berjalan proses identifikasi, dokumentasi, dan implementasi dari kebijakan aturan penggunaan informasi dan fasilitas pengelolaan aset organisasi.
C.8.1.4 Pengembalian aset	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah menerapkan prosedur pengembalian aset secara formal dari organisasi di saat pemutusan hubungan kerja.

Tabel 4.4 Rekomendasi Kontrol Keamanan Pada C.8 Lanjutan

Kontrol Keamanan	Rekomendasi
C.8.2.1 Klasifikasi informasi	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah menerapkan pengklasifikasian (pengelompokkan) data informasi yang dapat diakses maupun yang tidak dapat diakses pengguna.
C.8.2.2 Pelabelan informasi	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan pelabelan pada aset organisasi dengan mengikuti prosedur dari negara.
C.8.2.3 Penanganan aset	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah diterapkannya prosedur penaganan aset baik informasi maupun aset pengelolaan informasi, yaitu melakukan pencadangan data aset informasi dan pemeliharaan dan perbaikan bagi aset pengelolaan informasi.
C.8.3.1 Manajemen media yang dapat dipindahkan	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah menerapkan prosedur pemindahan media yang dapat dipindahkan.
C.8.3.2 Pembuangan media	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah menerapkan prosedur pembuangan media secara formal oleh organisasi dengan mengikuti prosedur negara.
C.8.3.3 Transfer media fisik	Melindungi media yang berisi informasi dari akses yang tidak sah selama perjalanan transpotasi. Adapun panduan implementasi yang dapat dilakukan yaitu: Dalam transfer media fisik beberapa hal yang harus dipertimbangkan antara lain: a. Menggunakan transpotasi atau kurir yang dapat diandalkan dan disetujui oleh manajemen. b. Prosedur untuk memverifikasi kurir harus dikembangkan. c. Pengemasan barang harus dipastikan aman dan cukup untuk melindungi isi dari kerusakan fisik selama proses transit.

3. C.9 Kontrol akses

Tabel 4.5 Rekomendasi Kontrol Keamanan Pada C.9

Kontrol Keamanan	Rekomendasi
C.9.1.1 Kontrol akses	Organisasi harus menetapkan, mendokumentasikan dan meninjau serangkaian kebijkan kontrol akses sesuai dengan peraturan atau prosedur keamanan informasi. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Aturan atau kebijakan kontrol akses, hak akses, dan batasan yang sesuai untuk peran pengguna harus ditetapkan oleh pemilik aset, b. Memberikan pernyataan yang jelas tentang persyaratan bisnis yang harus dipenuhi oleh kontrol akses kepada penyedia dan pengguna layanan akses. c. Kebijakan kontrol akses harus berisikan: - Persyaratan keamanan aplikasi bisnis. - Kebijakan dalam penyebaran dan otorisasi informasi. - Konsistensi antara hak akses dan kebijakan klasifikasi informasi sistem dan jaringan. - Undang-undang yang signifikan dan perjanjian apapun yang berkaitan dengan layanan akses.

Tabel 4.5 Rekomendasi Kontrol Keamanan Pada C.9 Lanjutan

Kontrol Keamanan	Rekomendasi
	- Kebijakan pemisahan peran kontrol akses (permintaan akses, otorisasi akses, administrasi akses). - Kebijakan untuk otorisasi formal dalam permintaan akses. - Kebijakan peninjauan berkala atas hak akses - Kebijakan penghapusan hak akses, pengarsipan semua peristiwa penting terkait penggunaan dan pengelolaan identitas pengguna dan informasi otentikasi rahasia. - Kebijakan peran terhadap akses istimewa.
C.9.1.2 Akses ke jaringan dan layanan jaringan	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan pembatasan hak akses ke jaringan dan layanan jaringan berdasarkan tipe pengguna.
C.9.2.1 Pendaftaran dan pembatalan pendaftaran pengguna	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan prosedur pendaftaran pembuatan akun pengguna.
C.9.2.2 Penyediaan akses pengguna	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan penyediaan akses pengguna secara formal.
C.9.2.3 Manajemen hak akses istimewa	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan pembatasan dan pengendalian hak akses istimewa.
C.9.2.4 Pengelolaan informasi otentikasi rahasia pengguna	Melakukan pengontrolan alokasi informasi otentikasi rahasia secara formal proses manajemen. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Proses formal yang dimaksud mencakup persyaratan berikut yaitu: - Pengguna harus menandatangani sebuah perjanjian yang berisi kesanggupan dan kesepakatan pengguna untuk menyimpan informasi otentikasi rahasia dan menjaga informasi rahasia kelompok. - Menetepkan prosedur dalam memverifikasi identitas pengguna sebelum menyediakan pengganti yang baru. - Pengguna harus menjaga informasi otentikasi rahasianya, dengan mengubah password sementara disaat penggunaan pertama. - Informasi otentikasi rahasia sementara harus unik untuk individu dan tidak boleh bisa ditebak. - Pengguna harus mengakui penerimaan informasi otentikasi rahasia. - Pengubahan informasi otentikasi rahasia vendor default harus dilakukan setelah sistem atau perangkat lunak dipasangkan.
C.9.2.5 Tinjauan hak akses pengguna	Peninjauan hak akses secara berkala harus dilakukan secara berkala oleh pemilik aset. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Beberapa hal yang harus dipertimbangkan saat melakukan peninjauan hak akses yaitu: - Hak akses pengguna harus ditinjau secara berkala dan setelah ada perubahan, seperti promosi, penurunan pangkat atau pemutusan hubungan kerja. - Hak akses pengguna harus ditinjau dan dialokasikan kembali saat berpindah dari satu peran ke peran lainnya dalam organisasi yang sama. - Otorisasi untuk hak akses istimewa harus ditinjau pada interval yang lebih sering. - Alokasi hak istimewa harus diperiksa secara berkala untuk memastikan bahwa hak istimewa yang tidak sah belum diperoleh

Tabel 4.5 Rekomendasi Kontrol Keamanan Pada C.9 Lanjutan

Kontrol Keamanan	Rekomendasi
	- Perubahan pada akun istimewa harus dicatat untuk ditinjau secara berkala.
C.9.2.6 Penghapusan atau penyesuaian hak akses	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan penghapusan hak akses terhadap pengguna yang sudah dilakukan saat pemutusan kerja.
C.9.3.1 Penggunaan informasi otentikasi rahasia	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan penyaranan terhadap pengguna untuk mengikuti praktik organisasi dalam penggunaan informasi otentikasi rahasia.
C.9.4.1 Pembatasan akses informasi	Membatasi akses ke informasi dan fungsi sistem aplikasi sesuai dengan kebijkan kontrol akses. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Pembatasan akses harus didasarkan pada persyaratan aplikasi bisnis individu dan sesuai dengan kebijakan kontrol akses yang ditentukan. Hal yang perlu dipertimbangkan untuk mendukung persyaratan pembatasan akses - Menyediakan menu untuk mengontrol akses ke fungsi sistem aplikasi. - Mengontrol data mana yang dapat diakses oleh pengguna tertentu. - Mengontrol hak akses pengguna, misalnya membaca, menulis, menghapus, dan mengeksekusi. - Mengendalikan hak akses aplikasi lain. - Membatasi informasi yang terkandung dalam output. - Menyediakan kontrol akses fisik atau logis untuk isolasi aplikasi sensitif, aplikasi data, atau sistem.
C.9.4.2 Prosedur log-on yang aman	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan prosedur log-on yang aman.
C.9.4.3 Sistem manajemen kata sandi	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan manajemen kata sandi yang berkualitas.
C.9.4.4 Penggunaan program utilitas istimewa	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan pembatasan dalam penggunaan program utilitas istimewa oleh pengguna tertentu.
C.9.4.5 Kontrol akses ke kode sumber program	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan pembatasan hak akses sumber kode program oleh orgaisasi.

4. C.10 Kritografi

Tabel 4.6 Rekomendasi Kontrol Keamanan Pada C.10

Kontrol Keamanan	Rekomendasi
C.10.1.1 Kebijakan penggunaan kontrol kriptografi	Kebijakan penggunan kontrol kriptografi harus dibuat, diterapkan dan dikembangkan Adapun panduan implementasi yang dapat dilakukan yaitu: a. Dalam mengembangkan kebijakan kriptografi, terdapat hal yang perlu dipertimbangkan yaitu: - Melindungi informasi bisnis dalam pendekatan manajemen terhadap penggunaan kontrol kriptografi di seluruh organisasi. - Mengidentifikasi hasil penilaian resiko dan tingkat perlindungan dengan mempertimbangkan jenis kekuatan dan kualitas algoritma enkripsi yang diperlukan. - Menerapkan penggunaan enkripsi dalam melindungi informasi yang diperoleh dari media seluler atau perangkat yang dapat dipindahkan atau jalur komunikasi. - Pendekatan manajemen kunci, termasuk metode untuk menangani perlindungan kriptografi kunci dan pemulihan informasi terenkripsi jika kunci hilang, disusupi, atau rusak. - Peran dan tanggung jawab, misalnya siapa yang bertanggung jawab atas implementasi kebijakan dan manajemen kunci. - Standar yang akan diadopsi untuk implementasi yang efektif di seluruh organisasi. - Dampak penggunaan informasi terenkripsi pada kontrol yang mengandalkan pemeriksaan konten (mis deteksi *malware*). b. Dalam menerapkan kebijakan kriptografi terdapat beberapa hal yang perlu dipertimbnagkan yaitu: - Peraturan dan batasan nasional yang berlaku pada penggunaan teknik kriptografi di dunia dan masalah arus lintas batas informasi terenkripsi.
C.10.1.2 Manejemen kunci	Mengembangkan dan mengimplementasikan kebijakan tentang penggunaan, perlindungan, dan masa pakai kunci kriptografi. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Kebijakan manajemen kunci juga harus dibuat dan dikembangkan. Adapun kebijakan ini berisikan persyaratan untuk mengelola kunci kriptografi melalui seluruh siklus hidupnya termasuk menghasilkan, menyimpan, mengarsipkan, mengambil, mendistribusikan, menghentikan dan menghancurkan kunci. b. Memilih dan menerapkan algoritme kriptografi, panjang kunci, dan dengan penerapan yang sesuai dan benar. Dalam menerapkan manajemen kunci yang tepat memerlukan proses yang aman untuk menghasilkan, menyimpan, mengarsipkan, mengambil, mendistribusikan, menghentikan dan menghancurkan kunci kriptografi. c. Melindungi semua kunci kriptografi dari pengubahan, kehilangan, dan penggunaan yang tidak sah. Sehingga peralatan yang digunakan untuk menghasilkan, menyimpan dan kunci arsip harus dilindungi secara fisik. d. Penggunaan sistem manajemen kunci harus berdasarkan seperangkat standar, prosedur, dan keamanan yang disepakati organisasi. e. Menentukan tanggal aktivasi dan penonaktifan kunci untuk mengurangi kemungkinan penggunaan yang tidak tepat, sehingga kunci hanya dapat digunakan untuk jangka waktu yang ditentukan dalam kebijakan manajemen kunci terkait.

5. C.11 Keamanan fisik dan lingkungan

Tabel 4.7 Rekomendasi Kontrol Keamanan Pada C.11

Kontrol Keamanan	Rekomendasi
C.11.1.1 Perimeter keamanan fisik	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan perimeter keamanan fisik pada lingkungan pengelolaan informasi.
C.11.1.2 Kontrol entri fisik	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan pengontrolan entri fisik,
C.11.1.3 Mengamankan kantor, ruangan, dan fasilitas	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat pemanfaatan fasilitas pengamanan kantor, ruangan, dan fasilitas pengola informasi.
C.11.1.4 Melindungi dari ancaman eksternal dan lingkungan	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat pemanfaatan fasilitas perlindungan dari ancaman eksternal dan lingkungan.
C.11.1.5 Bekerja di area yang aman	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan prosedur bekerja di area yang aman.
C.11.1.6 Area pengiriman dan pemuatan	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan prosedur bekerja di area yang aman.
C.11.2.1 Penempatan dan perlindungan peralatan	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapanpenempatan dan perlindungan peralatan yang sesuai dan aman.
C.11.2.2 Utilitas pendukung	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penyediaan fasilitas batre cadangan/UPS dan genset sebagai bentuk perlindungan dari adanya gangguan kegagalan daya.
C.11.2.3 Keamanan kabel	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan pengamanan kabel yang sesuai dan aman.
C.11.2.4 Pemeliharaan peralatan	Memelihara peralatan dengan benar agar ketersediaan dan integritas peralatan tersebut dapat berkelanjutan. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Memelihara peralatan sesuai dengan interval servis yang direkomendasikan pemasok dan spesifikasi. b. Pemeliharaan hanya boleh dilakukan oleh personel resmi.

Tabel 4.7 Rekomendasi Kontrol Keamanan Pada C.11 Lanjutan

Kontrol Keamanan	Rekomendasi
	c. Menyimpan semua catatan dari kesalahan yang dicurigai atau yang sebenarnya, dan semua pemeliharaan preventif dan korektif. d. Melakukan pengendalian yang tepat ketika peralatan dijadwalkan untuk pemeliharaan, dengan mempertimbangkan apakah pemeliharaan ini dilakukan oleh personel di lokasi atau di luar organisasi; bila perlu, informasi rahasia harus dibersihkan dari peralatan atau personil pemeliharaan harus cukup bersih. e. Mematuhi semua persyaratan pemeliharaan yang dikenakan oleh polis asuransi. f. Memeriksa terlebih dahulu sebelum mengoperasikan kembali peralatan setelah pemeliharaannya.
C.11.2.5 Penghapusan aset	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan peraturan yang dilakukan saat penghapusan aset.
C.11.2.6 Keamanan peralatan dan aset di luar lokasi	Menerapkan keamanan pada aset di luar lokasi dengan mempertimbangkan berbagai kemungkinan resiko saat bekerja di luar. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Manajemen harus mengontrol penggunaan peralatan penyimpanan dan pemrosesan informasi apa pun di luar lokasi organisasi, baik peralatan yang dimiliki oleh organisasi maupun peralatan yang dimiliki secara pribadi dan digunakan atas nama organisasi. b. Mempertimbangkan beberapa pedoman untuk melindungi peralatan di luar lokasi organisasi yang diantaranya: - Tidak boleh meninggalkan peralatan dan media yang diambil dari tempat organisasi tanpa pengawasan di tempat umum. - Memperhatikan instruksi pabrik untuk melindungi peralatan setiap saat, contohnya melindungi peralatan terhadap paparan medan elektromagnetik yang kuat. - Melakukan kontrol saat di luar lokasi seperti kerja jarak jauh. - Mempertahankan log ketika peralatan di luar lokasi dipindahkan di antara individu yang berbeda atau pihak eksternal guna melacak keberadaan peralatan. c. Memperhitungkan dan menentukan pengendalian yang tepat untuk resiko yang mungkin terjadi.
C.11.2.7 Pembuangan atau penggunaan kembali peralatan secara aman	Melakukan verifikasi terhadap semua item peralatan yang berisi media penyimpanan untuk memastikan setiap data sensitif dan perangkat lunak berlisensi sudah dihapus dengan aman sebelum dibuang. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Memverifikasi peralatan untuk memastikan apakah media penyimpanan ditampung atau tidak, sebelum dibuang atau digunakan kembali. b. Memusnahkan media penyimpanan yang berisi informasi rahasia atau berhak cipta secara fisik, c. Informasi yang terdapat pada peralatan harus dihapus atau ditimpa menggunakan teknik agar keaslian informasi tidak dapat diambil alihalih menggunakan fungsi hapus atau format standar.
C.11.2.8 Peralatan pengguna tanpa pengawasan	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan prosedur perlindungan peralatan di area yang tanpa pengawasan.
C.11.2.9 Bersihkan meja dan kebijakan layer yang jelas	Membuat kebijakan *clear desk* dan *clear screen* yang jelas Adapun panduan implementasi yang dapat dilakukan yaitu: a. Kebijakan *clear desk* dan *clear screen* harus mempertimbangkan beberapa hal seperti klasifikasi informasi persyaratan hukum, kontrak, resiko terkait serta aspek budaya dari organisasi. Hal yang dapat dilakukan yaitu: - Mengkunci informasi bisnis yang sensitif atau kritis, di dalam brankas bila tidak diperlukan, apalagi saat kantor sedang sepi.

Tabel 4.7 Rekomendasi Kontrol Keamanan Pada C.11 Lanjutan

Kontrol Keamanan	Rekomendasi
	- Komputer dan terminal harus dibiarkan mati atau dilindungi dengan layar dan penguncian keyboard mekanisme yang dikendalikan oleh kata sandi, token, atau mekanisme otentikasi pengguna serupa ketika tanpa pengawasan dan harus dilindungi dengan kunci, kata sandi, atau kontrol lain saat tidak digunakan. - Mencegah penggunaan mesin fotokopi dan teknologi reproduksi lainnya yang tidak sah

6. C.12 Operasi keamanan

Tabel 4.8 Rekomendasi Kontrol Keamanan Pada C.12

Kontrol Keamanan	Rekomendasi
C.12.1.1 Prosedur operasi terdokumentasi	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat dokumentasi prosedur operasi.
C.12.1.2 Manajemen perubahan	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat pengendalian terhadap manajemen perubahan.
C.12.1.3 Manajemen kapasitas	Organisasi harus melakukan pemantauan, penyetelan, dan membuat proyeksi kebutuhan kapasitas dari penggunaan sumber daya di masa mendatang. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Mengidentifikasi persyaratan kapasitas dengan mempertimbangkan kekritisan bisnis yang bersangkutan dengan sistem. b. Membuat proyeksi kebutuhan kapasitas masa depan dengan mempertimbangkan kebutuhan bisnis, sistem baru, dan tren saat ini menyesuaikan kemampuan pemprosesan informasi organisasi. c. Menerapkan kotrol detektif untuk menunujukkan masalah yang terjadi pada waktunya. d. Memantau pemanfaatan sumber daya sistem utama. e. Menyediakan kapasitas yang cukup dengan meningkatkan kapasitas atau dengan mengurangi permintaan.
C.12.1.4 Pemisahan lingkungan pengembangan, pengujian, dan operasional	Organisasi harus membuat lingkungan pengembangan, pengujian, dan erosionalal secara terpisah, untuk meminimalisir resiko akses tidak sah atau perubahan lingkungan operasional. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Mengidentifikasi dan mengimpelementasikan tingkat pemisahan antara lingkungan operasional, pengujian, dan pengembangan untuk mencegah masalah operasional. Beberapa hal yang dapat dilakukan yaitu: - Menetapkan dan mendokumentasikan aturan dalam pemindahan perangkat lunak dari pengembangan ke status operasional. - Menjalankan perangkat lunak pengembangan dan operasional pada sistem atau prosesor komputer yang berbeda dan di domain atau direktori yang berbeda. - Melakukan pengujian perubahan terlebih dahulu pada sistem operasional dan aplikasi dalam lingkungan pengujian atau staging, sebelum diterapkan pada sistem operasional. - Menetapkan aturan larangan melakukan pengujian pada sistem operasional, kecuali dalam keadaan yang darurat atau mengharuskan. - Kompiler, editor, dan alat pengembangan atau utilitas sistem lainnya tidak boleh diakses dari sistem operasional bila tidak diperlukan. - Pengguna harus menggunakan profil pengguna yang berbeda untuk sistem operasional dan pengujian, dan menu harus menampilkan pesan identifikasi yang sesuai untuk mengurangi resiko kesalahan.

Tabel 4.8 Rekomendasi Kontrol Keamanan Pada C.12 Lanjutan

Kontrol Keamanan	Rekomendasi
	- Data sensitif tidak boleh disalin ke lingkungan sistem pengujian kecuali kontrol yang setara disediakan untuk sistem pengujian.
C.12.2.1 Kontrol terhadap malware	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan pengontrolan terhadap *malware.*
C.12.3.1 Cadangan informasi	Organisasi harus melakukan pengambilan salinan cadangan informasi, perangkat lunak, dan gambar sistem harus secara teratur sesuai dengan kebijakan cadangan yang disepakati. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Menetapkan kebijakan pencadangan yang berisi prosedur organisasi dalam melakukan pencadangan informasi, perangkat lunak dan sistem. b. Kebijakan pencadangan yang dibuat harus mencakup persyaratan penyimpanan dan perlindungan. c. Menyediakan fasilitas cadangan yang memadai agar semua informasi penting dan perangkat lunak dapat dipulihkan setelah bencana atau kegagalan media. d. Memantau prosedur operasional pelaksanaan pencadangan dan penanganan kegagalan jadwal *backup* untuk memastikan kelengkapan *backup* sesuai dengan kebijakan *backup*. e. Melakukan pengujian pada pengaturan pencadangan untuk sistem dan layanan individual secara teratur untuk memastikan f. Menentukan periode penyimpanan informasi bisnis penting harus ditentukan, dengan mempertimbangkan setiap: persyaratan salinan arsip untuk disimpan secara permanen.
C.12.4.1 Pencatatan peristiwa	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan pencatatan peristiwa yang disesuaikan dengan kebutuhan organisasi.
C.12.4.2 Perlindungan informasi log	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan pembatasan hak akses logging.
C.12.4.3 Log administrator dan operator	Pencatatan administrator sistem, aktivitas operator sistem, dan log harus dicatat, dilindungi dan tinjau secara teratur. Adapun panduan implementasi yang dapat dilakukan yaitu: Pemegang akun pengguna yang memiliki hak istimewa mungkin dapat memanipulasi log pada pemrosesan informasi fasilitas di bawah kendali langsung mereka, oleh karena itu perlu untuk melindungi dan meninjau log untuk dipelihara akuntabilitas untuk pengguna istimewa.
C.12.4.4 Sinkronisasi jam	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan penyinkronisasian jam/waktu sesuai dengan lokasi waktu organisasi.
C.12.5.1 Instalasi perangkat lunak operasional	Hal yang harus dilakukan bila organisasi memiliki aplikasi yang diunduh pada komputer, maka prosedur harus diterapkan dalam mengontrol instalasi perangkat lunak pada sistem operasional. Adapun panduan implementasi yang dapat dilakukan yaitu: - Membuat prosedur kontrol perubahan perangkat lunak pada sistem operasional dengan mempertimbangkan pedoman berikut: - Hanya administrator yang ahli dapat melakukan pembaruan perangkat lunak operasional, aplikasi, dan pustaka program. - Hanya kode yang dapat dieksekusi dan disetujui yang boleh disimpan oleh sistem operasional, dan bukan kode pengembangan atau kompiler. - Implementasi aplikasi dan perangkat lunak sistem operasi dapat dilakukan setelah ekstensif dan pengujian berhasil, baik dalam fungsi, keamanan, dan efek pada sistem lain.

Tabel 4.8 Rekomendasi Kontrol Keamanan Pada C.12 Lanjutan

Kontrol Keamanan	Rekomendasi
	- Menerapkan sistem kontrol konfigurasi untuk menjaga kontrol semua perangkat lunak yang diimplementasikan sebagai dokumen sistem, dan menerapkan strategi rollback sebelum perubahan diterapkan. - Mempertahankan versi perangkat lunak yang lama, sebagai tindakan darurat. - Memelihara log audit dari semua pembaruan ke perpustakaan program operasional. - Mengarsipkan semua informasi dan parameter yang diperlukan, prosedur, rincian konfigurasi dan perangkat lunak pendukung selama data disimpan dalam arsip erangkat lunak versi lama.
C.12.6.1 Manajemen kerentanan teknis	Organisasi harus memperoleh informasi kerentanan teknis dari sistem informasi dengan tepat waktu, dan kerentanan teknis tersebut harus di evaluasi dengan langkah-langkah yang tepat. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Tindakan yang tepat dan tepat waktu harus diambil dalam menanggapi identifikasi potensi teknis kerentanan dengan membangun proses manajemen yang efektif. Berikut yang dapat dilakukan dalam membangun manajemen yang efektif yaitu: - Menetapkan peran dan tanggung jawab yang terkait dengan teknis manajemen kerentanan, termasuk pemantauan kerentanan, penilaian resiko kerentanan, patching, pelacakan aset dan tanggung jawab koordinasi yang diperlukan. - Mengidentifikasi sumber daya informasi yang akan digunakan untuk mengidentifikasi kerentanan teknis yang signifikan dan untuk memelihara kesadaran tentang mereka. - Menentukan garis waktu untuk bereaksi terhadap pemberitahuan kerentanan teknis yang berpotensi signifikan. - Mengidentifikasi resiko terkait dan tindakan yang akan diambil. - Tindakan yang diambil harus dilakukan sesuai dengan kontrol yang terkait dengan manajemen perubahan atau dengan mengikuti prosedur respons insiden keamanan informasi, tergantung pada seberapa mendesak kerentanan teknis perlu ditangani. - Log audit harus disimpan untuk semua prosedur yang dilakukan. - Memantau proses manajemen kerentanan teknis dan mengevaluasi secara teratur dalam rangka menjamin efektivitas dan efisiensinya. - Menangani sistem beresiko tinggi terlebih dahulu. - Mengevaluasi resiko yang berkaitan dengan kerentanan yang diketahui dan menentukan tindakan detektif dan korektif yang tepat, apabila terdapat masalah yang tidak ada penanggulangan yang sesuai.
C.12.6.2 Pembatasan instalasi perangkat lunak	Hal yang harus dilakukan bila organisasi memiliki aplikasi yang diunduh pada komputer, maka prosedur harus ditetapkan dan diterapkan dalam aturan yang mengatur isntalasi perangkat lunak. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Organisasi harus menetapkan dan menerapkan kebijakan yang ketat tentang jenis perangkat lunak yang boleh dipasang oleh pengguna b. Organisasi harus mengidentifikasi jenis instalasi perangkat lunak apa yang diizinkan (misalnya pembaruan dan patch keamanan untuk perangkat lunak yang ada) dan jenis instalasi apa yang dilarang (misalnya perangkat lunak yang hanya untuk penggunaan pribadi dan perangkat lunak yang silsilahnya berkaitan dengan keberadaan berpotensi berbahaya tidak diketahui atau dicurigai). c. Hak-hak istimewa ini harus diberikan dengan memperhatikan peran pengguna yang bersangkutan.

Tabel 4.8 Rekomendasi Kontrol Keamanan Pada C.12 Lanjutan

Kontrol Keamanan	Rekomendasi
C.12.7.1 Pengendalian audit sistem sistem informasi	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan pengendalian oleh organisasi saat adanya audit sistem informasi dalam bentuk pengawasan dan pendampingan.

7. C.13 Keamanan komunikasi

Tabel 4.9 Rekomendasi Kontrol Keamanan Pada C.13

Kontrol Keamanan	Rekomendasi
C.13.1.1 Kontrol jaringan	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan pengelolaan dan pengendalian jaringan.
C.13.1.2 Keamanan layanan jaringan	Melakukan identifikasi mekanisme keamanan, tingkat layanan, dan persyaratan manajemen dari semua layanan jaringan, yang disertakan dalam perjanjian layanan jaringan. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Menentukan dan memantau secara rutin mengenai kemampuan penyedia layanan jaringan dalam mengelola layanan dengan cara yang aman serta menyepakati untuk melakukan audit. b. Mengidentifikasi pengaturan keamanan yang diperlukan untuk layanan tertentu, seperti fitur keamanan, tingkat layanan dan persyaratan manajemen.
C.13.1.3 Segregasi dalam jaringan	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat pengelompokkan penggunaan akses internet.
C.13.2.1 Kebijakan dan prosedur transfer informasi	Menyediakan kebijakan, prosedur, dan kontrol transfer secara formal untuk melindungi transfer informasi melalui penggunaan semua jenis fasilitas komunikasi. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Membuat dan menerapkan prosedur dan kontrol disaat menggunakan fasilitas komunikasi yang harus mempertimbangkan hal berikut: - Prosedur mengenai perlindungan informasi yang ditransfer dari penyadapan, penyalinan, modifikasi, salah rute dan penghancuran. - Prosedur mengenai deteksi dan perlindungan terhadap malware yang mungkin ditularkan melalui penggunaan komunikasi elektronik. - Prosedur mengenai perlindungan informasi elektronik sensitif yang dikomunikasikan berupa: sebuah lampiran. - Kebijakan yang menerangkan penggunaan fasilitas komunikasi yang dapat diterima. - Himbauan kepada personel, pihak eksternal, dan tanggung jawab pengguna lain untuk tidak membahayakan organisasi, misalnya melalui pencemaran nama baik, pelecehan, peniruan identitas, penerusan surat berantai, tanpa izin pembelian, dll. - Penggunaan teknik kriptografi misalnya untuk melindungi kerahasiaan, integritas dan keaslian informasi. - Kebijakan penyimpanan dan pembuangan untuk semua korespondensi bisnis, termasuk pesan, sesuai dengan dengan undang-undang dan peraturan nasional dan lokal yang signifikan. Kontrol dan pembatasan yang terkait dengan penggunaan fasilitas komunikasi, misalnya penerusan otomatis surat elektronik ke alamat surat eksternal.

Tabel 4.9 Rekomendasi Kontrol Keamanan Pada C.13 Lanjutan

Kontrol Keamanan	Rekomendasi
C.13.2.2 Perjanjian tentang transfer informasi	Membuat perjanjian yang membahas transfer informasi bisnis yang aman antara organisasi dan pihak ketiga. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Perjanjian transfer informasi harus mencakup hal-hal berikut: - Tanggung jawab manajemen untuk mengendalikan dan memberitahukan pengiriman, pengiriman dan penerimaan. - Prosedur untuk memastikan ketertelusuran dan non-penyangkalan. - Standar teknis minimum untuk pengemasan dan transmisi. - Perjanjian escrow. - Standar identifikasi kurir. - Tanggung jawab dan kewajiban jika terjadi insiden keamanan informasi, seperti kehilangan data. - Penggunaan sistem pelabelan yang disepakati untuk informasi sensitif atau kritis, memastikan bahwa arti dari label segera dipahami dan informasi tersebut dilindungi dengan tepat. - Standar teknis untuk merekam dan membaca informasi dan perangkat lunak. - Kontrol khusus apa pun yang diperlukan untuk melindungi item sensitif, seperti kriptografi. - Memelihara lacak balak untuk informasi selama transit. - Tingkat kontrol akses yang dapat diterima. b. Menetapkan dan memelihara kebijakan, prosedur dan standar untuk melindungi informasi dan media fisik dalam perjalanan.
C.13.2.3 Pesan elektronik	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan jalur pesan elektronik.
C.13.2.4 Perjanjian kerahasiaan atau kerahasiaan	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan dalam mengidentifikasi, meninjau dan mendokumentasi perjanijian kerahasiaan atau kerahasiaan yang dikelola oleh organisasi.

8. C.14 Akusisi, pengembangan, dan pemeliharaan

Tabel 4.10 Rekomendasi Kontrol Keamanan Pada C.14

Kontrol Keamanan	Rekomendasi
C.14.1.1 Persyaratan keamanan sistem informasi	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan pengendalian dalam pengelolaan tentang persyaratan keamanan sistem informasi yang disesuaikan dengan kebutuhan organisasi.
C.14.1.2 Mengamankan layanan aplikasi di jaringan publik	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan fasilitas pengamanan layanan aplikasi pada jaringan publik.
C.14.1.3 Melindungi transaksi layanan aplikasi	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan perlindungan transaksi layanan aplikasi antara organisasi dengan mitra kerjasama.
C.14.2.1 Kebijakan pembangunan yang aman	Menetapkan dan menerapkan aturan dalam pengembangan perangkat lunak dan sistem. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Menyediakan pengembangan yang aman dalam membangun layanan, arsitektur, perangkat lunak, dan sistem. b. Mempertimbangkan aspek-aspek dalam kebijakan pembangunan yang aman berupa: - Keamanan lingkungan pembangunan. - Panduan tentang keamanan dalam siklus hidup pengembangan perangkat lunak, keamanan dalam metodologi pengembangan

Tabel 4.10 Rekomendasi Kontrol Keamanan Pada C.14 Lanjutan

Kontrol Keamanan	Rekomendasi
	- perangkat lunak dan pedoman pengkodean yang aman untuk setiap bahasa pemrograman yang digunakan. - Persyaratan keamanan dalam tahap desain. - Pos pemeriksaan keamanan dalam tonggak proyek. - Penyimpanan yang aman. - Keamanan dalam kontrol versi. - Pengetahuan keamanan aplikasi yang diperlukan. - Kemampuan pengembang untuk menghindari, menemukan dan memperbaiki kerentanan. c. Menggunakan teknik pemrograman yang aman baik dalam pengembangan baru maupun dalam skenario penggunaan kembali kode di mana standar yang diterapkan untuk pengembangan mungkin tidak diketahui atau tidak konsisten dengan saat ini praktik terbaik. d. Jika pengembangan dialihdayakan, organisasi harus memperoleh jaminan bahwa pihak eksternal mematuhi dengan aturan ini untuk pengembangan yang aman.
C.14.2.2 Prosedur pengendalian perubahan sistem	Prosedur pengendalian perubahan sistem dalam siklus hidup pengembangan harus dikendalikan secara formal. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Mendokumentasikan dan menegakkan prosedur pengendalian perubahan secara formal untuk memastikan integritas sistem, aplikasi dan produk, dari tahap desain awal hingga semua upaya pemeliharaan selanjutnya. b. Melakukan proses dokumentasi, spesifikasi, pengujian, kontrol kualitas dan implementasi terkelola dalam pengenalan sistem baru dan perubahan besar pada sistem. c. Melakukan proses penilaian resiko, analisis dampak perubahan dan spesifikasi: kontrol keamanan yang diperlukan.
C.14.2.3 Tinjauan teknis aplikasi setelah perubahan platform operasi	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan peninjauan teknis aplikasi kembali, saat terdapat perubahan platform.
C.14.2.4 Pembatasan perubahan pada paket perangkat lunak	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan pembatasan modifikasi pada paket perangkat lunak.
C.14.2.5 Prinsi-prinsip rekayasa sistem yang aman	Menetapkan, mendokumentasikan, memelihara, dan menerapkan prinsip-prinsip untuk sistem keamanan rekayasa dalam setiap upaya implementasi sistem informasi. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Menetapkan, mendokumentasikan, dan menerapkan prosedur rekayasa sistem informasi yang aman berdasarkan prinsip-prinsip rekayasa pada kegiatan rekayasa sistem informasi internal. b. Merancang keamanan ke dalam semua lapisan arsitektur (bisnis, data, aplikasi, dan teknologi) penyeimbangan kebutuhan akan keamanan informasi dengan kebutuhan akan aksesibilitas. c. Menganalisis teknologi baru untuk resiko keamanan dan meninjau desain terhadap pola serangan yang diketahui. d. Meninjau prinsip-prinsip dan prosedur rekayasa yang sudah ditetapkan secara teratur untuk memastikan bahwa mereka secara efektif berkontribusi pada peningkatan standar keamanan dalam proses rekayasa dan untuk memastikan bahwa mereka tetap *up to date* dalam hal memerangi setiap yang baru potensi ancaman dan tetap berlaku untuk kemajuan teknologi dan solusi yang diterapkan.

Tabel 4.10 Rekomendasi Kontrol Keamanan Pada C.14 Lanjutan

Kontrol Keamanan	Rekomendasi
	e. Menerapkan prinsip-prinsip rekayasa keamanan yang ditetapkan untuk *outsourcing* sistem informasi melalui kontrak dan perjanjian mengikat lainnya antara organisasi dan pemasok kepada siapa organisasi melakukan *outsourcing*.
C.14.2.6 Lingkungan pengembangan yang aman	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan lingkungan pengembangan yang aman.
C.14.2.7 Pengembangan yang dialihdayakan	Organisasi harus mengawasi dan memantau aktivitas pengembangan sistem yang dialihdayakan. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Mempertimbangkan beberapa hal dalam pengembangan sistem dialihdayakan, yang mencakup: - Pengaturan lisensi, kepemilikan kode dan hak kekayaan intelektual yang terkait dengan outsourcing konten. - Persyaratan kontrak untuk praktik desain, pengkodean, dan pengujian yang aman. - Penyediaan model ancaman yang disetujui untuk pengembang eksternal. - Pengujian penerimaan untuk kualitas dan keakuratan kiriman. - Penyediaan bukti bahwa ambang batas keamanan digunakan untuk menetapkan tingkat minimum yang dapat diterima dari kualitas keamanan dan privasi. - Penyediaan bukti bahwa pengujian yang memadai telah diterapkan untuk menjaga terhadap tidak adanya keduanya; konten berbahaya yang disengaja dan tidak disengaja pada saat pengiriman. - Pengaturan escrow, misalnya jika kode sumber tidak lagi tersedia. - Hak kontraktual untuk mengaudit proses dan kontrol pengembangan. - Dokumentasi yang efektif dari lingkungan pembangunan yang digunakan untuk membuat kiriman. - Organisasi tetap bertanggung jawab untuk mematuhi hukum yang berlaku dan efisiensi pengendalian verifikasi.
C.14.2.8 Pengujian keamanan sistem	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan pengujian fungsional keamanan sistem.
C.14.2.9 Pengujian penerimaan sistem	Menetapkan program pengujian penerimaan dan kriteria pada sistem informasi yang baru, *upgrade*, maupun versi baru. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Melakuka pengujian penerimaan sistem yang mencakup pengujian persyaratan keamanan informasi dan kepatuhan terhadap praktik pengembangan sistem yang aman. b. Melakukan pengujian pada komponen yang diterima dan sistem terintegrasi dengan memanfaatkan alat otomatis, seperti alat analisis kode atau pemindai kerentanan, dan harus memverifikasi remediasi keamanan cacat terkait. c. Melakukan pengujian dalam lingkungan pengujian yang realistis untuk memastikan bahwa sistem tidak akan memperkenalkan kerentanan terhadap lingkungan organisasi dan bahwa pengujian tersebut dapat diandalkan.
C.14.3.1 Perlindungan data uji	Memasimalkan pemilihan, pengendalian, dan perlindungan terhadap data uji. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Menghindari penggunaan data operasional yang berisi informasi pengenal pribadi saat pengujian pengujian. Namun jika organisasi menggunakan informasi pengenal pribadi asaat pengujian, maka semua detail dan konten sensitif harus dilindungi dengan menghapus atau memodifikasi.

Tabel 4.10 Rekomendasi Kontrol Keamanan Pada C.14 Lanjutan

Kontrol Keamanan	Rekomendasi
C.14.3.1 Perlindungan data uji	b. Melindungi data operasional dengan panduan berikut: - Prosedur kontrol akses, yang berlaku dalam sistem aplikasi operasional, juga harus berlaku dalam menguji sistem aplikasi. - Memiliki otorisasi terpisah setiap kali informasi operasional disalin ke lingkungan pengujian. - Mengahpus informasi operasional dari lingkungan pengujian segera setelah pengujian selesai menyelesaikan. - Mencatat penyalinan dan penggunaan informasi operasional untuk sebagai jejak audit.

9. C.15 Hubungan pemasok

Tabel 4.11 Rekomendasi Kontrol Keamanan Pada C.15

Kontrol Keamanan	Rekomendasi
C.15.1.1 Kebijakan keamanan informasi untuk hubungan pemasok	Organisasi harus menetapkan kebijakan keamanan informasi dalam hubungan pemasok yang menangani proses dan prosedur yang akan dilaksanakan oleh organisasi, serta proses dan prosedur yang harus pihak pemasok terapkan. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Kebijakan yang dibuat harus memuat mengenai jenis layanan, kompenen infrastruktur TI, yang boleh atau diizinkan oleh organisasi untuk diakses informasinya. b. Kebijakan yang dibuat harus memuat proses standar dan siklus hidup dalam mengelola hubungan pemasok. c. Kebijakan yang dibuat harus memuat persyaratan keamanan informasi dan jenis kewajiban yang berlaku bagi pemasok dalam melindungi informasi organisasi.
C.15.1.2 Mengatasi keamanan dalam perjanjian pemasok	Menetapkan dan mendokumentasikan perjanjian persyaratan keamanan informasi yang relevan. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Persyaratan keamanan informasi harus memuat deskripsi informasi yang disediakan dan metode penyediaan informasi. b. Persyaratan keamanan informasi harus memuat peraturan hukum dalam perlindungan data, hak kekayaan intelektual dan hak cipta. c. Persyartan keamanan informasi harus memuat aturan penggunaan informasi yang diperbolehkan dan yang tidak diperbolehkan. d. Persyaratan keamanan informasi harus memuat peraturan yang relevan dengan kontrak. Persyaratan keamanan informasi harus memuat perjanjian kewajiban pemasok untuk mematuhi persyaratan keamanan organisasi.
C.15.2.1 Pemantauan dan peninjauan layanan pemasok	Pemantauan dan peninjauan layanan pemasok harus memastikan bahwa persyaratan keamanan informasi dan kondisi perjanjian dipatuhi dan bahwa insiden dan masalah keamanan informasi dikelola dengan baik. Adapun panduan implementasi yang dapat dilakukan yaitu: a. memantau tingkat kinerja layanan untuk memverifikasi kepatuhan terhadap perjanjian. b. meninjau laporan layanan yang dihasilkan oleh pemasok dan mengatur pertemuan kemajuan rutin sesuai kebutuhan oleh kesepakatan. c. melakukan audit terhadap pemasok, dalam hubungannya dengan penelaahan atas laporan auditor independen, jika tersedia, dan tindak lanjut atas masalah yang teridentifikasi. d. memberikan informasi tentang insiden keamanan informasi dan meninjau informasi ini sebagaimana diperlukan oleh perjanjian dan setiap pedoman dan prosedur pendukung. e. meninjau jejak audit pemasok dan catatan peristiwa keamanan informasi, masalah operasional, kegagalan, penelusuran kesalahan dan gangguan terkait dengan layanan yang diberikan. f. menyelesaikan dan mengelola setiap masalah yang teridentifikasi.

Tabel 4.11 Rekomendasi Kontrol Keamanan Pada C.15 Lanjutan

Kontrol Keamanan	Rekomendasi
C.15.2.1 Pemantauan dan peninjauan layanan pemasok	g. meninjau aspek keamanan informasi dari hubungan pemasok dengan pemasoknya sendiri.
C.15.2.2 Mengelola perubahan pada layanan pemasok	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan pengelohan perubahan pada layanan pemasok jika terjadi penggunaan layanan yang tidak cocok untuk dipakai.

10. C.16 Manajemen insiden keamanan informasi

Tabel 4.12 Rekomendasi Kontrol Keamanan Pada C.16

Kontrol Keamanan	Rekomendasi
C.16.1.1 Tanggung jawab dan prosedur	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penanggung jawab dan prosedur manajemen insisden keamanan informasi.
C.16.1.2 Melaporkan peristiwa	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat saluran manajemen yang dapat dihubungi.
C.16.1.3 Melaporkan kelemahan keamanan informasi	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan pelaporan kelemahan keamanan informasi.
C.16.1.4 Penilaian dan keputusan tentang peristiwa keamanan informasi	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat proses penilaian atau penanggapan yang dilakukan organisasi.
C.16.1.5 Tanggapan terhadap insiden keamanan informasi	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan prosedur yang sesuai.
C.16.1.6 Belajar dari insiden keamanan informasi	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan proses evaluasi oleh organisasi.
C.16.1.7 Pengumpulan bukti	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan prosedur yang dilakukan dalam pengumpulan bukti.

11. C.17 Aspek keamanan informasi dari manajemen kelangsungan bisnis

Tabel 4.13 Rekomendasi Kontrol Keamanan Pada C.17

Kontrol Keamanan	Rekomendasi
C.17.1.1 Merencanakan kesinambungan keamanan informasi	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan upaya perencanaan dalam menjaga kesinambungan keamanan informasi.
C.17.1.2 Menerapkan kontinuitas keamanan informasi	Menerapkan kontrol dalam memastika tingkat kesinambungan yang diperlukan untuk keamanan informasi selama situasi yang merugikan. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Menyediakan struktur manajemen yang memadai dalam mempersiapkan, mengurangi, dan menanggapi gangguan keamanan sistem informasi. b. Menyediakan personel yang tanggap insiden dengan tanggung jawab, wewenang, dan kompentensi yang diperlukan dalam mengelola insiden keamanan informasi. c. Mendokumentasikan rencana, mengembangkan dan menyetujui prosedur tanggapan dan pemulihan dengan merincikan proses organisasi dalam mengelola peristiwa insiden keamanan informasi,
C.17.1.3 Memverifikasi, meninjau, dan mengevaluasi, kesinambungan keamanan informasi	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan proses verifikasi peninjauan dan pengevaluasi kesinambungan keamanan informasi.
C.17.2.1 Ketersediaan fasilitas pemprosesan informasi	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan fasilitas redudansi yang cukup.

C.18 Kepatuhan

Tabel 4.14 Rekomendasi Kontrol Keamanan Pada C.18

Kontrol Keamanan	Rekomendasi
C.18.1.1 Identifikasi peraturan perundang-undangan dan persyaratan kontrak yang berlaku	Semua undang-undang legislatif yang relevan, peraturan, persyaratan kontrak dan pendekatan organisasi untuk memenuhi persyaratan ini harus secara eksplisit diidentifikasi, didokumentasikan dan terus diperbarui untuk setiap sistem informasi dan organisasi. Adapun panduan implementasi yang dapat dilakukan yaitu: - Kontrol khusus dan tanggung jawab individu untuk memenuhi persyaratan ini juga harus didefinisikan dan didokumentasikan. - Manajer harus mengidentifikasi semua undang-undang yang berlaku untuk organisasi mereka untuk memenuhi persyaratan untuk jenis bisnis mereka. - Jika organisasi menjalankan bisnis di negara lain, manajer harus mempertimbangkan kepatuhan di semua negara yang relevan.
C.18.1.2 Hak kekayaan intelektual	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan prosedur tidak bertentangan dengan hak kekayaan intelektual.

Tabel 4.14 Rekomendasi Kontrol Keamanan Pada C.18 Lanjutan

Kontrol Keamanan	Rekomendasi
C.18.1.3 Perlindungan catatan	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan prlindungan catatan yang sesuai.
C.18.1.4 Privasi dan perlindungan informasi pengenal pribadi	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan perlindungan privasi dan Informasi pribadi.
C.18.1.5 Regulasi kontrol kriptografi	Menggunakan kontrol kriptografi sesuai dengan perjanjian, undang-undang, dan peraturan. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Mempertibangkan pembatasan impor atau ekspor perangkat keras dan lunak komputer dalam kinerja fungsi kriptografi. b. Mempertimbangkan pembatasan impor dan ekspor perangkat keras dan lunak komputer yang dirancang dalam penambahan fungsi kriptografi. c. Mempertimbangkan pembatasan penggunaan enkripsi. d. Mempertimbangkan metode akses wajib atau pilihan oleh otoritas negara terhadap informasi yang dienkripsi pada perangkat keras maupun lunak dalam memberikan kerahasiaan konten. e. Mencari penasihat hukum untuk memastiknan kepatuhan undang-undang dan peraturan yang relevan.
C.18.2.1 Tinjauan indipenden terhadap keamanan informasi	Melakukan peninjauan independen dalam interval yang sudah direncanakan, baik dalam pengendalian tujuan keamanan informasi, kontrol keamanan informasi, kebijakan keamanan informasi, proses dan prosedur keamanan informasi. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Manajemen harus memulai tujuan independen untuk memastikan kesesuaian, kecukupan, dan keefektifan yang berkelanjutan dalam mengelola keamanan informasi. b. Peninjauan harus mencakup penilaian peluang untuk perbaikan dan kebutuhan dalam perubahan pendekatan keamanan informasi, termasuk tujuan kebijakan dan kontrol. c. Peninjauan harus dilakukan oleh individu yang independen, terampil dan berpengalaman, dan mengkhususkan diri dalam kegiatan tinjauan tersebut. d. Mencatat dan melaporakan hasil tinjauan kepada manajemen, yang disertai dengan pemeliharaan laporan tinjauan. e. Mempertimbangkan untuk melakukan perbaikan (korektif), jika terdapat tinjauan yang tidak sesuai atau terpenuhi dengan arahan untuk keamanan informasi.
C.18.2.2 Kepatuhan terhadap kebijakan dan standar keamanan	Melakukan peninjauan kepatuhan pemprosesan informasi dan prosedur dalam wilayah tanggung jawab dengan kebijakan keamanan, sesuai dengan standar dan keamanan lainnya secara berkala. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Mengidentifikasi proses peninjauan persyaratan keamanan informasi yang terpenuhi dalam kebijakan standar dan peraturan lain keamanan informasi. b. Mempertimbangkan alat pengukuran dan pelaporan otomatis untuk tinjauan regular yang efesien. c. Saat ditemukan ketidakpatuhan dalam hasil tinjauan, maka manajer harus mengidentifikasi penyebab ketidakpatuhan, mengevaluasi kebutuhan tindakan dalam mencapai kepatuhan, melakukan perbaikan yang tepat, dan melakukan peninjauan tindakan perbaikan untuk memverifikasi keefektifan tindakan perbaikan yang dibuat. d. Mengidentifikasi kekurangan atau kelemahan dari tindakan perbaikan yang dibuat.

Tabel 4.14 Rekomendasi Kontrol Keamanan Pada C.18 Lanjutan

Kontrol Keamanan	Rekomendasi
C.18.2.3 Tinjauan kepatuhan teknis	Meninjau kepatuhan kebijakan dan standar keamanan sistem informasi secara teratur dalam pelaksanaan teknis. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Melakukan peninjauan kepatuhan teknis dengan bantuan alat otomatis atau manual. b. Menyediakan individu yang berkompeten dan berwewenang untuk melakukan peninjauan kepatuhan teknis.