Jurnal Teknik Informatika (JUTIF)
Vol. 4, No. 4, August 2023, pp. 733-750

DOI: https://doi.org/10.52436/1.jutif.2023.4.4.689
p-ISSN: 2723-3863
e-ISSN: 2723-3871

INFORMATION SYSTEM SECURITY AUDIT USING ISO/IEC 27002:2013 AT UNIVERSITY OF XXX

Rusmala Santi[1], Aminullah Imal Alfresi[2], Betha Octariana[3]

[1,2,3]Information Systems, Faculty of Science and Technology, Universitas Negeri Islam Raden Fatah, Indonesia
Email: [1]rusmalasanti_uin@radenfatah.ac.id, [2]aminullah@radenfatah.ac.id, [3]bethaoctariana12@gmail.com

(Article Received: November 15, 2022: Revision: Desember 10, 2022; Published: August 18, 2023)

Abstract

Information system security audit to find out how the current information system security process is implemented, whether it has been implemented in accordance with information security management system standards. The purpose of this study is to examine the suitability of the current information system security process with the ISO/IEC 27002:2013 security standard and to assess the level of capability and maturity of information system security at university of XXX. This audit research resulted in the finding that the information system security process at university of XXX is currently not in accordance with the ISO/IEC 27002:2013 security standard and is at level 2 (managed) with a capability level value of 1,96 and a maturity level of 2,34.

Keywords: *Information System Security, ISO/IEC 27002:2013.*

AUDIT KEAMANAN SISTEM INFORMASI MENGGUNAKAN ISO/IEC 27002:2013 PADA UNIVERSITAS XXX

Abstrak

Audit keamanan sistem informasi untuk mengetahui bagaimana proses keamanan sistem informasi yang berjalan saat ini, apakah sudah diimplementasikan sesuai dengan standar sistem manajemen keamanan informasi. Tujuan penelitian ini untuk memeriksa kesesuaian antara proses keamanan sistem informasi yang berjalan saat ini dengan standar keamanan ISO/IEC 27002:2013 dan menilai berapa besar tingkat kemampuan dan kematangan keamanan sistem informasi pada universitas XXX. Penelitian audit ini menghasilkan temuan bahwa proses kemanan sistem informasi pada universitas XXX saat ini belum sesuai dengan standar keamanan ISO/IEC 27002:2013 dan berada pada level 2 *(managed)* dengan nilai tingkat kemampuan 1,96 dan tingkat kematangan 2,34.

Kata kunci: *Audit, Keamanan Sistem Informasi, ISO/IEC 27002:2013.*

1. PENDAHULUAN

Audit merupakan kegiatan dalam mengumpulkan dan memeriksa bukti mengenai proses kerja yang sedang berlangsung pada suatu organisasi, untuk menentukan dan membuat laporan apakah proses kerja saat ini sudah sesuai dengan kebijakan yang sudah ditentukan atau tidak [1]. Audit dapat membantu organisasi dalam mengidentifikasi masalah yang berpotensi dapat membahayakan aset organisasi, baik berbentuk harta, benda, data, maupun sumber daya manusia yang ada pada organisasi, karena audit merupakan metode yang dapat digunakan dalam hal mengukur dan memvalidasi data [2]. Terdapat empat hal yang penting dalam auditing yaitu dilaksanakan dengan orang yang *independent*, terdapat bukti, mengacu pada pedoman, dan membuat laporan hasil audit [3].

Audit keamanan sistem informasi merupakan suatu alat atau perangkat dalam menentukan, mendapatkan, dan mengola setiap level keamanan dalam suatu organisasi [4]. Saat ini audit keamanan sistem informasi perlu dan penting untuk diimplementasikan di era serba canggih yang dapat mengancam kerahasiaan dan integritas data organisasi. Audit keamanan sistem informasi dapat dilakukan pada organisasi berskala besar seperti pada perguruan tinggi.

Universitas XXX merupakan lembaga besar yang menyangkut data banyak orang, sehingga diperlukan audit keamanan sistem informasi untuk memeriksa apakah keamanan sistem informasi saat ini sudah atau belum memenuhi keamanan berstandar sistem manajemen keamanan informasi yang berlaku. Selain itu penggunaan sistem informasi pada universitas XXX sebagai alat pembantu dalam mempemudah pengelolaan data, menuntut sistem

informasi tersebut harus dilengkapi dengan keamanan sistem informasi yang baik. Karena diketahui bahwa pernah terjadi peretasan *website* remunerasi pada tahun 2017, yang mengakibatkan terkendalanya akses ke *website* tersebut oleh para pegawai dan dosen. Selain itu diketahui pula bahwa pernah beberapa kali terjadinya permasalahan jaringan yang mengakibatkan terhambatnya aktivitas akademik.

Maka dari itu akan dilakukan penelitian audit ini untuk memeriksa kondisi dan menilai seberapa besar nilai serta tingkat kemampuan dan kematangan keamanan sistem informasi yang berjalan saat ini. Sehingga dibutuhkan pedoman yang selaras dengan ruang lingkup keamanan sistem informasi, yaitu seperti standar ISO/IEC 27002:2013 yang membahas mengenai manajemen keamanan informasi dalam bidang IT, dimana tersedia 14 klausul yang berisi 35 kategori keamanan utama dengan 114 kontrol keamanan [5]. ISO/IEC 27002:2013 akan memberikan relomendasi yang disertai dengan panduan implementasi untuk organisasi, sehingga dapat mempermudah dalam melakukan perbaikan pada temuan proses keamanan sistem informasi yang belum sesuai.

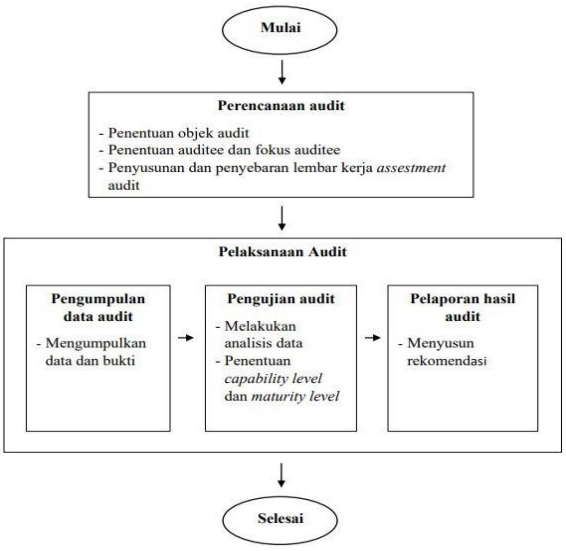
Hasil penelitian berupa temuan apakah keamanan sistem informasi saat ini sudah sesuai dengan standar keamanan ISO/IEC 27002:2013, sehingga akan menyediakan sebuah laporan audit yang berisi temuan audit dan rekomendasi terhadap kontrol keamanan informasi ISO/IEC 27002:2013 yang memerlukan perbaikan. Penelitian ini juga akan memberikan informasi mengenai seberapa besar nilai serta level tingkat kemampuan *(capability level)* dan tingkat kematangan *(maturity level)* keamanan sistem informasi menggunakan CMMI *(Capability Maturity Model Integration)* dengan level kemampuan (0-3) dan level kematangan (1-5).

2. METODE PENELITIAN

Metode penelitian yang digunakan yaitu metode penelitian evaluasi *(evaluation research).* Metode evaluasi adalah suatu penelitian yang dimana dalam prosesnya bersifat mengevaluasi suatu objek yang dapat berupa pelaksanaan suatu program, yang bertujuan untuk mengukur dan menentukan apakah program tersebut sudah sesuai dengan apa yang diharapkan [6]. Fokus penelitian ini adalah evaluasi proses yaitu evaluasi yang bertujuan untuk melakukan penilaian kinerja kerja [7]. Metode pengumpulan data pada penelitian ini terbagi menjadi dua yaitu data primer dan sekunder. Data primer merupakan data yang didapatkan secara langsung saat kegiatan audit, melalui wawancara, pengisian lembar kerja assessment audit, dan observasi.

Sedangkan data sekunder merupakan data yang diperoleh secara tidak langsung, seperti melalui studi kepustakaan [8]. Tahapan pada penelitian ini dibuat berdasarkan gabungan antara tahapan audit dan tahapan metode evaluasi yang disesuaikan dengan kebutuhan penelitian. Tahapan penelitian dapat dilihat pada gambar 1.

1. Tahapan perencanaan audit, dimana auditor akan melakukan penentuan objek yang akan diaudit, menentukan auditee dan fokus auditee, serta menyusun lembar kerja *assessment* audit.
2. Tahapan pelaksanaan, dimana auditor akan melakukan pengumpulan data dan bukti yang telah diperoleh dari pengisian lembar kerja *assessment* audit, melakukan analisis data dengan memeriksa kesesuaian antara implementasi proses organisasi saat ini dengan implementasi ISO/IEC 27002:2013, memberikan penilaian *capability level* (0-3) dan *maturity level* (1-5) pada masing-masing jawaban yang telah dikumpulkan.
3. Tahapan pelaporan hasil audit, dimana auditor akan melakukan pembuatan laporan hasil audit yang berisikan temuan audit dan rekomendasi untuk temuan audit yang belum sesuai dengan implementasi ISO/IEC 27002:2013.



Gambar 1. Tahapan Penelitian

3. HASIL DAN PEMBAHASAN

Pada bagian ini berisi gambaran penjelasan lebih lanjut mengenai tahapan penelitian yang dilakukan yaitu dari tahapan perencanaan audit sampai dengan tahapan pelaporan audit.

3.1. Perencanaan Audit

Pada sub bab ini akan menjeleaskan mengenai penentuan objek audit, penentuan auditee dan fokus auditee, serta penyusunan dan penyebaran lembar kerja *assessment* audit.

3.1.1. Penentuan Objek Audit

Objek yang dipilih untuk diaudit adalah keamanan sistem informasi pada universitas XXX.

3.1.2. Penentuan Auditee dan Fokus Auditee

Penentuan fokus auditee merupakan salah satu bagian penting yang harus dilakukan, dimana auditor akan melakukan pemetaan terhadap auditee dan fokus auditee berdasarkan pedoman peran dan tanggung jawab manajemen aset informasi pada ISO 27001 [9]. Pemetaan auditee dan fokus auditee dapat dilihat pada tabel 1.

Tabel 1. Auditee Charter

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

3.1.3. Penyebaran Lembar Kerja *Assessment* Audit

Lembar kerja *assessment* menyajikan pertanyaan dari masing-masing kontrol keamanan ISO/IEC 27002:2013 yang jumlah pertanyaannya disesuaikan dengan pernyataan (standar) pada kontrol keamanan ISO/IEC 27002:2013. Pertanyaan tersebut dapat dijawab dengan memberikan pernyataan Iya/Tidak dan disertai dengan penjelasan implementasi yang dilakukan oleh organisasi saat ini. Lembar kerja *assessment* ini juga dilengkapi dengan keterangan penanggung jawab masing-masing fokus auditee yang disertai dengan tanda tangan auditee, sebagai bentuk persetujuan dan pertanggungjawaban bahwa kesesuaian auditee dan fokus auditee yang diberikan benar dan keseuaian jawaban pertanyaan pada lembar kerja tersebut dibuat dengan sebenar-benarnya sehingga dapat dipertanggunggjawabkan. Setelah lembar kerja *assessment* disusun, maka dilanjutkan dengan membagikannya pada auditee dan fokus auditee yang sudah ditentukan.

3.2. Pelaksanaan Audit

Pada sub bab ini akan menjeleaskan mengenai pengumpulan data audit, pengujian audit, dan pelaporan hasil audit.

3.2.1. Pengumpulan data dan bukti Audit

Berikut adalah contoh hasil pengumpulan data pada lembar kerja *assessment* audit pada C.5 Kebijakan keamanan informasi yang dapat dilihat pada tabel 2.

Tabel 2. Contoh Hasil Lembar Kerja *Assessment* Audit

C.5 Kebijakan Keamanan Informasi			
Kategori keamanan utama	**Kontrol keamanan**	**Implementasi**	**Keterangan bukti**
C.5.1 Arahan manajemen untuk keamanan informasi	C.5.1.1 Kebijakan untuk keamanan informasi	Kebijakan keamanan informasi berupa SOP dalam bentuk dokumen *online* dan belum diterbitkan secara formal, masih bersifat umum, dan belum lengkap berdasarkan standar kebijakan SMKI.	Tersedianya dokumen SOP pada *website* pustipd
	C.5.1.2 Tinjauan kebijakan untuk keamanan informasi	Peninjauan kebijakan keamanan saat ini dilakukan dengan menyesuaikan dinamika dan kebutuhan organisasi pada waktu tertentu, dan belum dilakukan secara berkala.	Tidak ada

3.2.2. Pengujian Audit

Setelah melakukan pengumpulan data audit, selanjutnya melakukan tahapan pengujian audit yang terdiri dari analisis data dan penentuan *capability level* dan *maturity level* untuk masing-masing kluasul ISO/IEC 27002:2013 pada universitas XXX. Analisis data, dilakukan dengan menganalisis kesesuaian antara jawaban implementasi masing-masing kontrol keamanan saat ini dengan ketentuan standar ISO/IEC 27002:2013 serta penilaian *capability level* (0-3) dan *maturity level* (1-5) pada CMMI. Setelah memberikan penilaian, selanjutnya dapat diperoleh nilai rata-rata *capability level* dan

maturity level pada masing-masing kontrol keamanan (kk) ISO/IEC 27002:2013. Berikut contohperhitungan nilai *capability level* dan *maturity level* pada kontrol keamanan klausul C.5 yaitu:

$$\bar{x}\ capability\ kk = \frac{\Sigma\ nilai\ jawaban}{n\ pertanyaan} \quad (1)$$

$$\bar{x}\ capability\ C.5.1.1 = \frac{2+2+2+2}{4} = \frac{8}{4} = 2$$

$$\bar{x}\ capability\ C.5.1.2 = \frac{2}{1} = 2$$

$$\bar{x}\ maturity\ kk = \frac{\Sigma\ nilai\ jawaban}{n\ pertanyaan} \quad (2)$$

$$\bar{x}\ maturity\ C.5.1.1 = \frac{2+2+2+2}{4} = \frac{8}{4} = 2$$

$$\bar{x}\ maturity\ C.5.1.2 = \frac{2}{1} = 2$$

Berikut contoh tabel hasil perhitungan dari penilaian *capability level* dan *maturity level* serta analisis kesesuaian dari ISO/IEC 27002:2013 pada kontrol keamanan klasul C.5 Kebijakan keamanan informasi yang dapat dilihat pada tabel 3.

Tabel 3. Contoh Hasil Lembar Kerja *Assessment* Audit

Implementasi saat ini	Implementasi ISO/IEC 27002:2013	Sudah/ Belum sesuai	Nilai CL	Nilai ML
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.	Tersedianya dokumen SOP pada *website* pustipd	Belum sesuai	2	2
Peninjauan kebijakan keamanan saat ini dilakukan dengan menyesuaikan dinamika dan kebutuhan organisasi pada waktu tertentu, dan belum dilakukan secara berkala.	Tidak ada	Belum sesuai	2	2

a. Penentuan *capability level* dan *maturity level*, dilakukan dengan mencari rata-rata nilai *capability level* dan *maturity level* pada kategori keamanan utama terlebih dahulu. Berikut contoh perhitungan rata-rata *capability level* dan *maturity level* kategori keamanan utama C.5.1 pada klausul C.5 yaitu:

$$\bar{x}\ capability\ kku = \frac{\Sigma\ nilai\ capability\ kk}{n\ kk} \quad (3)$$

$$\bar{x}\ capability\ C.5.1 = \frac{2+2}{2} = \frac{4}{2} = 2$$

$$\bar{x}\ maturity\ kku = \frac{\Sigma\ nilai\ maturity\ kk}{n\ kk} \quad (4)$$

$$\bar{x}\ maturity\ C.5.1 = \frac{2+2}{2} = \frac{4}{2} = 2$$

Setelah rata-rata nilai *capability level* dan *maturity level* kategori keamanan utama diperoleh, maka selanjutnya yaitu mencari nilai rata-rata masing masing klausul. Sedangkan untuk menentukan tingkat *capability level* dan *maturity level* dengan menyesuaikan hasil rata-rata nilai klausul dengan skala interval pada CMMI. Berikut contoh perhitungan nilai *capability level* dan *maturity level* pada klausul C.5 yaitu:

$$\bar{x}\ cl\ klausul = \frac{\Sigma\ nilai\ capability\ kku}{n\ kku} \quad (5)$$

$$\bar{x}\ cl\ C.5 = \frac{2}{1} = 2$$

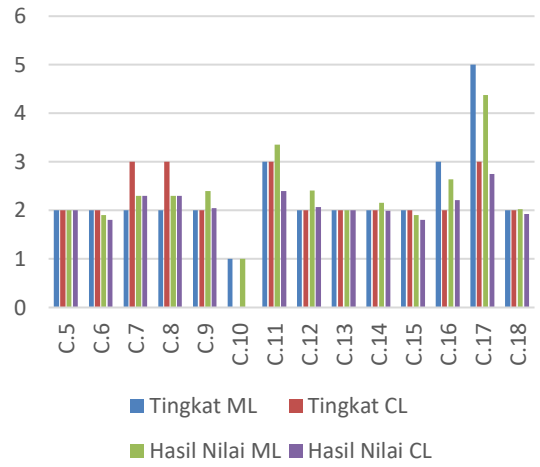
$$\bar{x}\ ml\ klausul = \frac{\Sigma\ nilai\ maturity\ kku}{n\ kki} \quad (6)$$

$$\bar{x}\ ml\ C.5 = \frac{2}{1} = 2$$

Setelah diperoleh rata-rata nilai *capability level* dan *maturity level* untuk klausul C.5 maka didapatkan tingkat level keduanya sama-sama berada pada level 2 yaitu *managed*. Perhitungan di atas berlaku sama untuk mencari nilai *capability leve*l dan *maturity level* pada semua klausul lainnya. Berikut adalah rekapitulasi hasil penilaian *capability level* dan *maturity level* klausul ISO/IEC 27002:2013 pada universitas XXX yang dapat dilihat pada tabel 4 dan gambar 2.

Tabel 4. Rekapitulasi Hasil Penilaian

Klausul	Hasil nilai CL	Level CL	Hasil nilai ML	Level ML	Keterangan CL/ML
C.5	2	2	2	2	*Managed*
C.6	1,8	2	1,9	2	*Managed*
C.7	2,16	2	2,30	2	*Managed*
C.8	2,3	3	2,3	2	*Defined/ Managed*
C.9	2,05	2	2,4	2	*Managed*
C.10	0	0	1	1	*Incomplete /Initial*
C.11	2,40	3	3,35	3	*Defined*
C.12	2,07	2	2,41	2	*Managed*
C.13	2	2	2	2	*Managed*
C.14	1,99	2	2,16	2	*Managed*
C.15	1,80	2	1,9	2	*Managed*
C.16	2,21	2	2,64	3	*Managed/ Defined*
C.17	2,75	3	4,38	5	*Defined/ Optimizing*
C.18	1,93	2	2,03	2	*Managed*
Rata-Rata	**1,96**	**2**	**2,34**	**2**	***Managed***



Gambar 2. Grafik Rekapitulasi Penilaian

Setelah mengetahui masing-masing nilai capability level dan maturity level untuk setiap klausul, maka dapat diperoleh besar nilai keseluruhan masing-masing capability level dan maturity level untuk keamanan sistem informasi pada universita XXX menggunakan standar ISO/IEC 27002:2013 yaitu sebagai berikut:

$$\bar{x}\ capability\ level = \frac{\Sigma\ nilai\ capability\ klausul}{n\ klausul}$$

$$\bar{x}\ capability\ level = \frac{27{,}46}{14} = 1{,}96$$

$$\bar{x}\ maturity\ level = \frac{\Sigma\ nilai\ maturity\ klausul}{n\ klausul}$$

$$\bar{x}\ maturity\ level = \frac{32{,}77}{14} = 2{,}34$$

Dari hasil penilaian di atas maka disimpulkan bahwa besar nilai keamanan sistem informasi pada universitas XXX menggunakan ISO/IEC 27002:2013 yaitu untuk nilai capability level sebesar 1,96 sedangkan untuk maturity level sebesar 2,34 dan sama-sama berada pada level 2 *(Managed)*.

b. Pelaporan hasil audit, merupakan media yang digunakan untuk mengkomunikasikan hasil audit kepada pihak-pihak yang berkeepentingan dengan maksud menyediakan informasi bagi pengambil keputusan bagi pengambil keputusan oleh manajemen terkait temuan audit, kesimpulan dan rekomendasi hasil penugasan audit. Pada pelaporan hasil audit ini, rekomendasi yang diberikan mengacu pada dokumen standar ISO/IEC 27002:2013 [10]. Rekomendasi adalah saran dari pemeriksaan berdasarkan hasil pemeriksaan yang ditunjukkan kepada orang atau badan yang berwewenang untuk melakukan tindakan atau perbaikan [11]. Berikut rekomendasi yang diberikan pada kontrol keamanan untuk masing-masing klausul yaitu:

1. C.5 Kebijakan keamanan informasi

Rekomendasi untuk klausul C.5 dapat dilihat pada tabel 5.

Tabel 5. Rekomendasi 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 formal 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. - 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. d. Kebijakan 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 atau jika terjadi perubahan yang signifikan terjadi untuk 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 mencakup penilaian peluang untuk perbaikan kebijakan dan pendekatan organisasi mengelola keamanan informasi dalam menanggapi perubahan terhadap lingkungan organisasi, keadaan bisnis, kondisi hukum atau

lingkungan teknis.
c. Tinjauan kebijakan untuk keamanan informasi harus mempertimbangkan hasil tinjauan manajemen.

2. C.6 Organisasi keamanan informasi
Rekomendasi untuk klausul C.6 dapat dilihat pada tabel 6.

Tabel 6. Rekomendasi 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: Keamanan informasi harus diintegrasikan ke dalam metode manajemen proyek organisasi untuk memastikan bahwa resiko keamanan informasi diidentifikasi dan ditangani sebagai bagian dari proyek.
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: Saat menggunakan perangkat seluler, perhatian khusus harus diberikan untuk memastikan bahwa informasi bisnis tidak dikompromikan. a. 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 langkah-langkah 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.*

3. C.7 Keamanan sumber daya manusia

Rekomendasi untuk klausul C.7 dapat dilihat pada tabel 7.

Tabel 7. Rekomendasi 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 tugasnya.
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 pendisiplina n	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.
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. 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., sehingga tetap sejalan dengan kebijakan dan prosedur organisasi, dan dapat juga bermanfaat bagi pegawai baru.

4. C.8 Manajemen Aset

Rekomendasi untuk klausul C.8 dapat dilihat pada tabel 8.

Tabel 8. Rekomendasi C.8

Kontrol keamanan	Rekomendasi
C.8.1.1 Invetarisasi aset	Implementasi yang berjalan 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.
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	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah menerapkan prosedur

dapat dipindahkan	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: - Menggunakan transpotasi atau kurir yang dapat diandalkan dan disetujui oleh manajemen. - Prosedur untuk memverifikasi kurir harus dikembangkan.

5. C.9 Kontrol akses
   Rekomendasi untuk klausul C.9 dapat dilihat pada tabel 9.

Tabel 9. Rekomendasi 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. - 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.
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.
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. - Alokasi hak istimewa harus diperiksa secara berkala untuk memastikan bahwa hak istimewa yang tidak sah belum diperoleh - 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	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan pembatasan akses yang aman.
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.

6. C.10 Kriptografi
   Rekomendasi untuk klausul C.10 dapat dilihat pada tabel 10.

Tabel 10. Rekomendasi 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. - 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.

7. C.11 Keamanan fisik dan lingkungan
   Rekomendasi untuk klausul C.11 dapat dilihat pada tabel 11.

Tabel 11. Rekomendasi 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	Implementasi yang berjalan saat ini sudah sesuai dengan pedoman implementasi ISO/IEC 27002:2013, yaitu sudah terdapat penerapan pemeliharaan terhadap peralatan pengelola informasi.
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.
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 alih-alih 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. 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.

8. C.12 Operasi keamanan
   Rekomendasi untuk klausul C.12 dapat dilihat pada tabel 12.

Tabel 12. Rekomendasi 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.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. Hal yang dilakukan menetapkan dan mendokumentasikan aturan dalam pemindahan perangkat lunak dari pengembangan ke status operasional.
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	Organisasi harus melakukan pengambilan

Cadangan informasi	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
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: a. 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.
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.
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.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.

9. C.13 Keamanan komunikasi
   Rekomendasi untuk klausul C.13 dapat dilihat pada tabel 13.

Tabel 13. Rekomendasi 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 744ensiti 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 perlindungan informasi elektronik 744ensitive 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. b. Menghimbau personel untuk tidak melakukan percakapan rahasia di depan umum atau melalui saluran komunikasi yang tidak aman.
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. - 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. 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.

10. C.14 Akusisi, pengembangan, dan pemeliharaan sistem

Rekomendasi untuk klausul C.14 dapat dilihat pada tabel 14.

Tabel 14. Rekomendasi 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: - Menyediakan pengembangan yang aman dalam membangun layanan, arsitektur, perangkat lunak, dan sistem. - 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 perangkat lunak dan pedoman pengkodean yang aman untuk setiap bahasa pemrograman yang digunakan.
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. 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. - 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. 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.

11. C.15 Hubungan Pemasok

Rekomendasi untuk klausul C.15 dapat dilihat pada tabel 15.

Tabel 15. Rekomendasi 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.
C.15.1.3 Rantai pasokan teknologi informasi dan komunikasi	Membuat perjanjian yang mencakup persyaratan dalam mengatasi resiko keamanan informasi seperti layanan teknologi informasi dan komunikasi, serta rantai pasokan produk. Adapun panduan implementasi yang dapat dilakukan yaitu: a. Menerapkan persyaratan keamanan informasi pada teknologi informasi dan komunikasi akuisisi produk atau layanan. b. Menerapkan proses pemantauan dan metode yang dapat memvalidasi informasi produk dan layanan teknologi informasi.
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.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.

12. C.16 Manajemen insiden keamanan informasi
    Rekomendasi untuk klausul C.16 dapat dilihat pada tabel 16.

Tabel 16. Rekomendasi 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 Pengumpula n 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.

13. C.17 Aspek keamanan informasi dari manajemen kelangsungan bisnis
    Rekomendasi untuk klausul C.17 dapat dilihat pada tabel 17.

Tabel 17. Rekomendasi C.17

Kontrol keamanan	Rekomendasi
C.17.1.1 Merencanakan kesinambunga n 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, kesinambunga n keamanan	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.

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.

14. C.18 Kepatuhan

Rekomendasi untuk klausul C.18 dapat dilihat pada tabel 18.

Tabel 18. Rekomendasi 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: a. Kontrol khusus dan tanggung jawab individu untuk memenuhi persyaratan ini juga harus didefinisikan dan didokumentasikan. b. Manajer harus mengidentifikasi semua undang-undang yang berlaku untuk organisasi mereka untuk memenuhi persyaratan untuk jenis bisnis mereka.
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.
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 metode akses wajib atau pilihan oleh otoritas negara terhadap informasi yang dienkripsi pada perangkat keras maupun lunak dalam memberikan kerahasiaan konten. d. 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. Mengidentifikasi kekurangan dari tindakan perbaikan yang dibuat.
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.

4. DISKUSI

Dengan melakukan penelitian audit keamanan sistem informasi pada universitas XXX, diperoleh informasi penting yaitu mengenai informasi bagaimana kondisi keamanan sistem informasi yang sedang berjalan saat ini untuk universitas XXX. Sehingga kedepannya diharapkan kondisi keamanan sistem infromasi yang belum berjalan sesuai dengan standar sistem manajemen keamanan informasi dapat diperbaiki sesuai dengan pedoman standar ISO/IEC 27002:2013. Hal ini bertujuan agar keamanan sistem informasi pada universitas XXX dapat berjalan jauh lebih baik dari sebelumnya, sehingga permasalahan yang pernah terjadi dapat diminimalisir.

Selain itu melalui penelitian ini baik untuk peneliti maupun pembaca juga mendapatkan informasi yang penting, berupa ilmu pengetahuan mengenai standar SMKI dengan beberapa jenis dan versi standar yang ada yaitu salah satunya standar ISO/IEC 27002:2013. Seperti yang diketahui menjadi perbedaan antara penelitian ini dengan penelitian sebelumnya yaitu terletak pada versi

ISO/IEC yang digunakan. Dimana pada penelitian sebelumnya standar yang digunakan yaitu ISO/IEC 27001:2005 yang menyajikan 11 kontrol keamanan yang disertai dengan beberapa rekomendasi [12].

Sedangkan pedoman standar yang digunakan pada penelitian ini yaitu ISO/IEC 27002:2013 yang menyajikan 14 kontrol keamanan yang disertai dengan rekomendasi dan panduan implementasi bagi organisasi. Maka dari itu dengan perkembangan edisi yang sebelumnya dengan yang sekarang menjadi nilai tambah untuk organisasi, agar lebih mudah mengimplementasikan standar ISO/IEC menggunakan versi ISO/IEC 27002:2013.

5. STUDI PUSTAKA

Pada bagian ini berisi mengenai beberapa teori yang mendukung dalam melakukan penelitian ini yaitu:

5.1. Audit Keamanan Sistem Informasi

Audit keamanan sistem informasi merupakan sebuah proses pemeriksaan yang dilakukan berdasarkan kebijakan atau standar keamanan yang telah ditetapkan, guna menentukan semua keadaan dari perlindungan yang ada dan untuk memverifikasi apakah perlindungan yang diberikan berjalan dengan baik atau tidak [4]. Audit keamanan sistem informasi dapat dikatakan sebagai aktivitas yang harus terus berjalan (kontinu), dimana dalam prosesnya terbagi menjadi dua putaran proses yaitu proses konfirmasi dan proses perbaikan.

5.2. Tujuan Audit Keamanan Sistem Informasi

Audit keamanan sistem informasi memiliki lima tujuan utama yaitu:

1. Untuk memeriksa atau mengamati kesesuaian baik itu kebijakan, pedoman, bakuan, serta prosedur keamanan yang sudah ditetapkan.
2. Untuk mengenali atau identifikasi kekurangan dan mengamati seberapa efektif kebijkan, bakuan, pedoman, serta prosedur yang sudah ditetapkan.
3. Untuk mengamati dan mempelajari kelemahan yang sudah ditetapkan
4. Untuk menganalisis hambatan keamanan yang ada, seperti masalah operasional, manajerial dan administrasi.
5. Untuk memberikan rekomendasi dan aksi perbaikan untuk peningkatan keamanan system informasi yang akan dating.

5.3. Tahapan Audit Keamanan Sistem Informasi

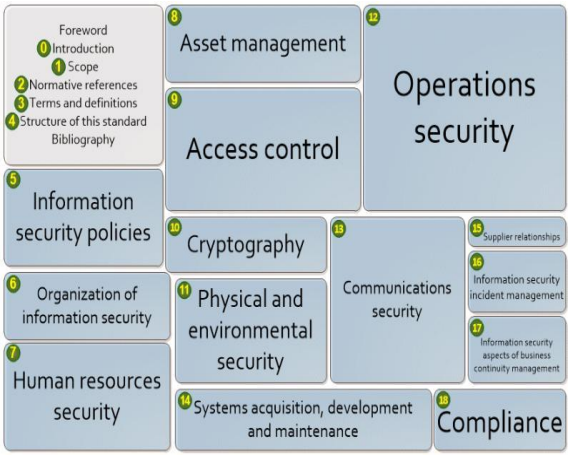
Audit keamanan sistem informasi memiliki 6 tahapan yaitu [4]:

1. Perencanaan audit
2. Pengumpulan data audit
3. Pengujian audit
4. Pelaporan hasil audit
5. Perlindungan atas data dan perangkat audit
6. Penambahan dan tindak lanjut

5.4. ISO/IEC 27002

ISO/IEC 27002 merupakan seri ISO/IEC 27000 yang sebelumnya adalah pembahruan dari ISO 17799, dimana standarisasi ini adalah keluaran dari dua organisasi internasional yaitu *International Organization for Standardization* (ISO) dan *International Electrotechnical Commission* (IEC). Standar ISO/IEC berisikan mengenai sejumlah standar *Information Security Management System* (ISMS) atau Sistem Manajemen Keamanan Informasi (SMKI). Standar ini merupakan seri ke 3 yang membahas mengenai kode praktik dari sistem manajemen keamanan sistem informasi. ISO/IEC 27002:2013 merupakan pedoman standarisasi yang menerangkan contoh implementasi keamanan informasi melalui bentuk-bentuk kontrol tertentu untuk mencapai sasaran kontrol yang ditetapkan. ISO/IEC 27002 pernah mengalami pembaruhan atau revisi dokumen, dimana sebelumnya disusun dan ditetapkan ke dalam dokumen panduan ISO/IEC 27002:2005 menjadi ISO/IEC 27002:2013.

Perbedaan diantara keduanya terletak pada struktur klausul yang dimilikinya, dimana berdasarkan dokumen panduan Badan Standar Nasional Tahun 2005, ISO/IEC 27002:2005 memiliki 11 klausul kontrol keamanan yang berisi 39 kategori keamanan utama [13]. Sedangkan berdasarkan Badan Standar Nasional Tahun 2013, ISO 27002:2013 memiliki 14 klausul yang berisi 35 kategori keamanan utama dengan 114 kontrol keamanan informasi [14]. Pada klausul ini pemberian kode klausul dimulai dari kode nomor C.5 sampai dengan C.18 dan nomor 0 sampai 4 merupakan pendahuluan penjelasan yang mencakup lingkup, referensi alternatif, istilah dan definisi, struktur dan standar yang tercantum pada dokumen ISO/IEC 27002:2013. Skema klausul ISO/IEC 27002:2013 dapat dilihat pada gambar 3.



Gambar 3. Skema Klausul ISO/IEC 27002:2013

5.5. *Capability Maturity Model Integration*

Capability Maturity Model Integration merupakan suatu proses perbaikan pendekatan yang memberikan organisasi unsur- unsur penting proses efektif yang pada akhirnya meningkatkan kinerja mereka [15]. Pada CMMI terdapat dua jenis level yaitu tingkat kemampuan *(capability level)* dan tingkat kematangan *(maturity level)* [16]. Tingkat kemampuan berlaku untuk peningkatan proses organisasi pencapaian di area proses individu secara bertahap yaitu 0-3. Sedangkan tingkat kematangan berlaku untuk peningkatan proses organisasi pencapaian tingkat kematangan diberbagai proses yaitu 1-5. Berikut adalah tabel perbandingan tingkat kemampuan dan kematangan yang dapat dilihat pada tabel 19.

Tabel 19. Perbandingan Tingkat Kemampuan dan Kematangan

Level	***Capability Level***	***Maturity Level***
0	*Incomplete*	
1	*Perfomed*	*Initial*
2	*Managed*	*Managed*
3	*Defined*	*Defined*
4		*Quantitavely Managed*
5		*Optimizing*

6. KESIMPULAN

Berdasarkan penelitian audit keamanan sistem informasi yang telah dilakukan pada universitas XXX, 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 universitas XXX, masih ditemukan beberapa implementasi yang belum sesuai maupun belum dilakukan berdasarkan ISO/IEC 27002:2013. Sehingga menghasilkan rekomendasi untuk beberapa kontrol keamanan yang memerlukan perbaikan sebagai bahan evaluasi untuk organisasi memperbaiki proses keamanan sistem informasi 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 pada universitas XXX yaitu sama-sama terletak pada level 2 *(managed)* dengan nilai *capability level* sebesar 1,96 dan *maturity level* sebesar 2,34. Hal ini menunjukkan bahwa baik proses tingkat kemampuan maupun tingkat kematangan dalam mengelola keamanan sistem informasi pada universitas XXX sudah menerapkan pengelolaan proses keamanan sistem informasi yang mengikuti prosedur yang berstandar dari organisasi sendiri dan masih bersifat umum, sehingga belum mengacu pada standar manajemen keamanan informasi secara khusus.

DAFTAR PUSTAKA

[1] E. Zuraidah, "Modul Audit Sistem Informasi Dan Tata Kelola," Makasar: Nusa Mandiri, 2019, pp. 1–95.

[2] F. Anggraini, *Audit Teknologi Sistem Intalasi Pengolahan Lumpur Tinja (IPTLT)*, 1st ed. Bandung: Kiblat Buku Utama, 2016.

[3] Y. Fiscal, "Pengaruh Pengalaman Kerja Dan Kompetensi Auditor Terhadap Kualitas Hasil Pemeriksaan (Studi Kasus pada Kantor BPKP Bandar Lampung)," *J. Akunt. dan Keuang.*, vol. 3, no. 1, 2012, doi: 10.36448/jak.v3i1.220.

[4] N. Ibrachim *et al*., *Bakuan Audit Keamanan Informasi Kemenpora*. Jakarta: Kementerian Pemuda dan Olahraga Republik Indonesia, 2012.

[5] M. Rizal, "Framework Audit IT," Karawang, 2016.

[6] S. Kantun, "Penelitian Evaluatif Sebagai Satu Model Penelitian Dalam Bidang Pendidikan," *Maj. Ilm. Din.*, vol. 37, no. 1, p. 15.

[7] D. Wirawan, *Evaluasi (Teori, Model, Metodologi, Standar, Aplikasi, dan Profesi)*, 3rd ed. Jakarta: Raja Grafindo Persada, 2016.

[8] J. A. H. Hardani. Ustiawaty, *Buku Metode Penelitian Kualitatif dan Kuantitatif*, 1st ed., no. April. Yogyakarta: CV Pustaka Imu Group, 2017.

[9] F. FISO 27001 Implementer, "Guideline for Roles & Responsibilities in Information Asset Management," 2009.

[10] Y. Yuliani, N. S. Lestari, R. S. Aisyah, K. M. Sofiani, and T. Alawiyah, "Pelaporan Hasil Audit Dan Tindak Lanjut Audit," Tasikmalaya, 2020.

[11] Undang-Undang RI, *Undang-Undang Republik Indonesia*. Indonesia, 2004, pp. 1–25.

[12] Y. Rahayu, "Audit Keamanan Informasi Simak Online Universitas Indo Global Mandiri Palembang Berdasarkan Standar ISO/IEC 27001:2005," 2018.

[13] Badan Standar Internasional, *Internasional Standard ISO / IEC 27002:2005*, vol. 2005. 2005.

[14] Bandar Standar Nasional, *Internasional Standard ISO / IEC 27002:2013*, Kedua., vol. 2013. 2013.

[15] A. Mewengkang, "Pemanfaatan Capability Maturity Model Integration Untuk Meningkatkan Kualitas Perangkat Lunak (Studi Kasus : Sistem Informasi Akademik Universitas Negeri Manado)," *Eng. Educ.*, vol. 7, no. 1, p. 6, 2019.

[16] Software Engineering Institute, *CMMI For Development Version 1.3*, 1.3., no. November. 2010.