BAB III

PELAKSANAAN KERJA MAGANG

3.1 Kedudukan dan Koordinasi

Selama melakukan praktek kerja magang di PT. United Tractors TBK., penulis berada di divisi CST (*Corporate Strategic Technology*) sebagai tim *IT Governance* and *Security* yang bertugas dan bertanggung jawab untuk. Pelaksanaan praktek kerja magang berada di bawah tanggung jawab Bapak Einto Rizad Ardii yang menjabat sebagai *staff IT Governance* and *Security* di PT. United Tractors Tbk.

Tugas utama yang dikerjakan selama mengikuti praktek kerja magang yaitu melakukan *supporting* dan implementasi *surveillance* ISO 27001 dan 20000 di PT. United Tractors Tbk, seperti memberikan *review* dan *improvement* dengan menggunakan *framework standard international* lainnya yaitu COBIT/ITIL pada dokumen *Policy*, SOP, *Data Collection*, dan membuat analisa *report* serta konten *awareness*, mempersiapkan dokumentasi *Surveillance* ISO 27001 dan 20000 dan melakukan *update* mengenai kajian terhadap *risk assessment* yang terkait dengan referensi dari *cybersecurity risk*. Selama menjalani masa praktek kerja magang, penulis berada di bawah tanggung jawab Bapak Einto Rizad Ardii yang menjabat sebagai *staff IT Governance* and *Security* di PT. United Tractors Tbk.

Untuk berkomunikasi atau berkoordinasi dengan supervisi, aplikasi yang digunakan selama melaksanakan program praktek kerja adalah aplikasi *WhatsApp* dan *E-mail*. Untuk *WhatsApp* dapat digunakan sebagai alat komunikasi, contoh pertanyaan mengenai tugas atau pekerjaan dan informasi lainnya. Sedangkan *E-mail* digunakan untuk mengirimkan file-file yang sudah selesai dikerjakan dan informasi lainnya.

3.2 Tugas dan Uraian Kerja Magang

3.2.1 Tugas yang dilakukan

Selama melakukan praktek kerja magang di PT. United Tractors TBK departemen CST (*Corporate Strategic Technology*) sebagai tim *IT Governance* and *Security* harus mengerjakan beberapa tugas dan tanggung jawab, diantaranya:

1. Melakukan *supporting* dan implementasi *surveillance* ISO 27001 dan 20000 di PT. United Tractors, seperti memberikan *review* dan *improvement* pada dokumen *Policy*, SOP, Form menggunakan *framework* COBIT, ITIL, dan NIST, membuat konten *awareness* ISO 27001 dalam bentuk infografis.
2. Mempersiapkan dokumentasi *surveillance* ISO 27001, ISO 20000 dan CAASM dalam bentuk membuat materi PPT.
3. Melakukan *update* mengenai kajian terhadap *risk assessment* yang terkait dengan referensi dari *cybersecurity risk*.

3.2.2 Uraian kerja magang

Pelaksanaan praktek kerja magang di PT. United Tractors sebagai *IT Governance* dan *Security* dilakukan dalam periode waktu 100 hari kerja dimulai dari tanggal 13 Juni 2022 sampai 30 November 2022. Aktivitas yang dilakukan sebagai besar yaitu melakukan *supporting* dan implementasi *surveillance* ISO 27001 dan 20000 dan melakukan *update* mengenai kajian terhadap *risk assessment*. Adapun uraian kerja magang dilakukan selama periode 123 hari kerja (6 bulan) dapat dilihat pada Tabel 3.1:

Table 3.1 Waktu Pelaksanaan Magang

No	Pekerjaan yang Dilakukan	Bulan (Minggu ke)	Waktu Mulai	Waktu Selesai
1	Briefing mengenai job description yang akan dilakukan selama magang	Juni (1)	13 Juni 2022	13 Juni 2022
2	Melakukan review dan improvement dokumen (Kebijakan, SOP)	Juni dan Juli (2-3 dan 1-2)	14 Juni 2022	15 Juli 2022
3	Membuat infografis awareness ISO (1)	Juli (3-4)	19 Juli 2022	29 Juli 2022
4	Mempelajari dokumen Kebijakan, SOP, IK, dan Form	Agustus (1-4)	1 Agustus 2022	24 Agustus 2022
5	Membuat pemetaan dokumen Kebijakan, SOP, IK, dan Form sesuai standard ISO	September (1-2)	25 Agustus 2022	8 September 2022
6	Membuat infografis awareness ISO (2)	September (3-4)	9 September 2022	22 September 2022
7	Mempelajari dan membuat materi ISO 27001:2022, CAASM dan ISO 27001;2019	Oktober (1)	23 September 2022	29 September 2022
8	Membuat pemetaan dokumen Kebijakan, SOP, Form yang sesuai standard NIST dan COBIT	Oktober (2-3)	4 Oktober 2022	14 Oktober 2022
9	Mempelajari dokumen risk assessment dan mengerjakan risk assessment	Oktober dan November (4 dan 1)	18 Oktober 2022	4 November 2022
10	Mempelajari materi tanggap insiden keamanan dan membuat SOP tanggap insiden keamanan dan persiapan insiden keamanan	November (2-3)	7 November 2022	30 November 2022

Pada hari pertama melaksanakan praktek kerja magang di PT.United Tractors Tbk, seorang divisi *IT Governance* dan *Security Intern* akan diberikan akses terkait dokumen-dokumen yang dapat mendukung seluruh pekerjaan magang yang akan dilakukan secara hybrid dan diberikan penjelasan mengenai tugas yang akan dikerjakan selama melaksanakan praktek kerja magang di PT. United Tractors Tbk. Disamping itu, selama berlangsungnya praktek kerja magang di PT. United Tractors Tbk terdapat beberapa pekerjaan yang telah dilakukan yaitu:

3.2.2.1 Membuat pemetaan dokumen Kebijakan, SOP, IK, dan Form sesuai standard ISO, COBIT, NIST

1) Dokumen PLC (Kebijakan)

   Berikut tabel 3.3 yang berisikan pemetaan dokumen kebijakan (PLC) yang sesuai dengan referensi standar internasional NIST, COBIT, dan ISO.

Table 3.2 Pemetaan Dokumen PLC sesuai referensi ISO, COBIT, NIST

No	Aktivitas	Kebijakan terkait	NIST	COBIT	ISO
1	Penggunaan perangkat lunak pribadi, perangkat keras pribadi, perangkat jaringan pribadi,	PLC 02 - Kebijakan penggunaan aset IT pribadi	ID.AM-3	DSS05.2	ISO A.8
2	Klasifikasi informasi, penanganan informasi rahasia, dan kepemilikan data di perusahaan.	PLC 03 - Klasifikasi informasi	ID. AM - 5, NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6	APO03.03, AP03.04, APO12.01, BAI04.02, BAI09.02	ISO A.8.2.1 dan ISO A.8.2.2
3	Penggunaan perangkat umum, email, akses internet dan login windows pc dan notebook	PLC 05 - Kebijakan penggunaan email dan internet	PR.DS-2, PR.DS-5, PR.AC-1, PR.PT-3 NIST SP 800-53 Rev. 4 SC-	APO01.06, DSS05.02, DSS06.06, DSS05.04, DSS05.07	ISO A.13.2.3, ISO A.9.1.2

No	Aktivitas	Kebijakan terkait	NIST	COBIT	ISO
			8, SC-11, SC-12		
4	Pengelolaan hak akses, password administrator, password super administrator, dan khusus bagi pihak ketiga	PLC 06 - Manajemen password	PR.AC-1, PR. DS -5	DSS05.04, DSS06.03, APO01.06, DSS05.07, DSS06.02	ISO A.9.2.6, ISO A.9.2.3, ISO A.9.4.3
5	Pedoman pemberian, peminjaman, dan penggunaan fasilitas komputer, printer dan handheld device	PLC 07 - Kebijakan pengelolaan computer, printer, dan handheld device	IS.AM-4, PR.AC-2, PR.AC-3, PR. MA-1, SP 800-53 Rev. 4 AC-20, SA-9	APO02.02, APO10.04, BAI03.10, BAI09.02, BAI09.03, DSS01.05, DSS01.02, DSS01.04, DSS05.05	ISO A.11.2.6, ISO A.6.2.1
6	Penggunaan software yang diizinkan dan legal di lingkungan perusahaan	PLC 08 - Kebijakan standard software	ID. GV-3	BAI02.01, MEA03.01, MEA03.04	ISO A.18.1.2
7	Pedoman dalam penyimpanan dan penggunaan HAKI	PLC 10 - Kebijakan Haki	ID. GV-3	BAI02.01, MEA03.01, MEA03.04	ISO A.18.1.2
8	Tata cara pembelajaran secara elektronik kepada user	PLC 13 - Kebijakan E-learning	PR.DS-4	APO13.01, BAI04.04	ISO A.12.1.3
9	Pedoman asuransi aset IT	PLC 14 - IT Insurance	ID.BE-5, PR. IP-9	APO12.06, DSS04.03, BAI03.02, DSS04.02	ISO A.17.1.1
10	tata cara pelaksanaan layanan corporate communication system dvisi CST	PLC 15 - Communication system	DE. DP-3, PR.DS-4	APO13.01, APO13.02, DSS05.02	ISO A.13.1 dan ISO A.12.1.3
11	Pedoman atas penggunaan mobile computing dan teleworking terkait	PLC 16 - Mobile computing dan teleworking	PR.AC-3	APO13.01, DSS01.04, DSS05.03	ISO A.6.2

No	Aktivitas	Kebijakan terkait	NIST	COBIT	ISO
	akses sistem informasi				
12	Standart konfigurasi perangkat IT (server, aplikasi, network device, dan perangkat IT lainnya)	PLC 17 - Standar konfigurasi perangkat IT	DE. DP-3	APO13.02, DSS05.02	ISO A.14.2.8
13	Standart audit trail/log seluruh jaringan, sistem, server dan komunikasi	PLC 18 - Kebijakan audit log	PR.PT-1, DE.AE-2, DE.CM-3, DE CM-7	APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02, DSS05.02, DSS05.05	ISO A.12.4, ISO A.13.1.1

2) Dokumen SOP

Berikut table 3.4 yang berisikan pemetaan dokumen SOP sesuai standar internasional NIST, COBIT, ISO

Table 3.3 Pemetaan Dokumen SOP sesuai referensi NIST, COBIT, ISO

No	Aktivitas	SOP terkait	NIST	COBIT	ISO
1	Pengendalian dokumen, Pengesahan, Perubahan/Revisi, Pendistrubisian Dokumen, Daftar induk dokumen, Sistem penomororan dokumen, Penanganan dokumen, Pembuatan dan penyusunan dokumen.	SOP 69 - Pengendalian Dokumen Catatan	PR. IP-4	APO13.01, DSS01.01, DSS04.07	ISO A.18.1.3
2	Peninjuan review audit internal, persiapan rencana audit, persiapan audit, pelaksanaan audit, temuan internal audit, monitoring hasil, dan hasil internal audit	SOP 70 - Internal Audit	PR.AC-7	DSS05.04, DSS05.10, DSS06.10	ISO A.9.3
3	Peserta manajemen review, agenda rapat manajemen terintegrasi, proses tinjauan manajemen	SOP 71 - Tinjauan Manajemen	PR.AC-1	DSS05.04, DSS06.03	ISO A.9.3
4	Cara melaksanakaan tindakan koreksi suatu ketidaksesuaian dan cara mencegah suatu ketidaksesuaian layanan teknologi keamanan informasi	SOP 72 - Ketidaksesuaian dan Perbaikan	PR.DS-5	APO01.06, DSS05.04, DSS05.07, DSS06.02	ISO A.10.1

No	Aktivitas	SOP terkait	NIST	COBIT	ISO
7	layanan kapasitas informasi, rencana penambahan kapasitas, waktu periodik informasi kapasitas.	SOP 75 - Demand and capacity management	PR.DS-4	APO13.01, BAI04.04	ISO A.12.1.3
16	Prosedur corrective maintenance perangkat jaringan, prosedur preventive maintenance jaringan	SOP 086 - pemeliharaan perangkat jaringan	PR.DS-8, PR.MA-1, PR.MA-2	DSS05.04, BAI03.10, BAI09.02, BAI09.03, DSS01.05, BAI10.01, BAI10.02, BAI10.03, BAI10.05	ISO A.11.2.4
17	Manajemen hak askes super administrator, pemberian hak akses super administrator sementara dan baru, pemberian atau perubahan hak akses operator, pemberian hak akses pihak ketiga, pemberian hak akses pengguna	SOP 087 - Pengelolaan hak akses	PR.DS-5, PR.AC-4	APO01.06, DSS05.04, DSS05.07, DSS06.02	ISO A.9.1.1, ISO A.9.2
18	Prosedur permintaan software berlisensi, instalansi softaware non-standard,	SOP 088 - Pengelolaan software berlisensi	PR. IP-1, ID.GV-3	BAI10.01, BAI10.02, BAI10.03, BAI10.05, BAI02.01, MEA03.01, MEA03.04	ISO A.12.6.2, ISO A.18.1.2
19	Penanganan informasi hardcopy dan softcopy, penerimaan informasi hardcopy dan softcopy, penggandaan informasi, serah terima tanggung jawba penyimpanan informasi apabila terjadi perubahan personil, peminjaman dokumen pihak ketiga, backup informasi, pemusnahan informasi.	SOP 089 - Penanganan informasi corporate	PR.AC-2, ID.AM-3, ID. GV-3, PR.IP-4	APO13.01, DSS01.04, DSS05.03, DSS05.02, BAI02.01, MEA03.01, MEA03.04, BAI01.06, BAI06.01	ISO A.11.2.7, ISO A.13.2.2, ISO A.18.1.3
20	Peminjaman aset, kehilangan aset, stok aset, mutasi aset, stock opname, penghapusan asset	SOP 090 - Pengelolaan aset IT	PR.AC-2, PR.DS-3, PR.MA-1	DSS01.04, DSS05.05, BAI09.03, BAI03.10, BAI09.02, BAI09.03, DSS01.05	ISO A.11.2.7
21	Serah terima fisik server, serah terima aplikasi, serah terima virtual machine, vulnerablity assesment,	SOP 091 - serah terima server	PR.DS-7	BAI03.08, BAI07.04	ISO A.12.1.4
22	Analisa permintaan aplikasi, analisa kelayakan sistem/aplikasi	SOP 094 - Permintaan aplikasi	PR.DS-5	APO01.06, DSS05.04,	ISO A.6.1.2

No	Aktivitas	SOP terkait	NIST	COBIT	ISO
		teknologi informasi		DSS05.07, DSS06.02	
23	Ketentuan pengembangan aplikasi, dokumen analisa kelayakan sistem, ketntuan versioning aplikasi, dan prosedur kajian	SOP 096 - Pengembangan aplikasi teknologi informasi	PR.AC-3	DSS05.04, DSS06.03	ISO A.6.2.1
24	Tata cara proses penyempurnaan aplikasi	SOP 097 - Penyempurnaan aplikasi	PR. IP-2	APO13.01, BAI03.01, BAI03.02, BAI03.03	ISO A.4.1.1
25	Proses permintaan asset IT	SOP 104 - Pengelolaan Perminataan IT	PR.AC-1, PR.AC-2, PR.DS-3, PR.MA-1, PR.DS-7	DSS05.04, DSS06.03, DSS01.04, DSS05.05, BAI09.03, BAI03.10, BAI09.02, DSS01.05, BA107.04, BA.103.08	ISO A.9.3, ISO A.11.2.5 dan ISO A.12.1.4

3) Dokumen Form

Berikut table 3.5 yang berisikan pemetaan dokumen form yang sesuai dengan standar internasional NIST, COBIT, ISO

Table 3. 4 Pemetaan Dokumen Form sesuai referensi NIST, COBIT, ISO

No	Nama Dokumen	NIST	COBIT	ISO
1	FRM 1 - Daftar Induk	PR. IP-4	APO13.01, DSS01.01, DSS04.07	ISO A.18.1.3
2	FRM 2 - Daftar Catatan	PR. IP-4	APO13.01, DSS01.01, DSS04.08	ISO A.18.1.3
3	FRM 3 - Daftar Distribusi Dokumen	PR. IP-4	APO13.01, DSS01.01, DSS04.09	ISO A.18.1.3
4	FRM 4 - Perubahan Dokumen	PR. IP-4	APO13.01, DSS01.01, DSS04.10	ISO A.18.1.3

No	Nama Dokumen	NIST	COBIT	ISO
5	FRM 5 - Jadwal kegiatan internal audit	PR.AC-7	DSS05.04, DSS05.10, DSS06.10	ISO A.9.3
6	FRM 6 - Temuan audit	PR.AC-7	DSS05.04, DSS05.10, DSS06.10	ISO A.9.3
7	FRM 7 - Rekapitulasi hasil internal audit	PR.AC-7	DSS05.04, DSS05.10, DSS06.10	ISO A.9.3
8	FRM 8 - Template Notulensi Tinjauan Management	PR.AC-1	DSS05.04, DSS06.03	ISO A.9.3
9	FRM 9 - Corrective action report	PR.DS-5	APO01.06, DSS05.04, DSS05.07, DSS06.02	ISO A.10.1
10	FRM 10 - SLA (Service level aggreement)	PR. IP-9	APO12.06, DSS04.03	ISO A.17
11	FRM 11 - Berita acara pengahncuran perangkat	PR.AC-2, PR.DS-3, PR.MA-1	DSS01.04, DSS05.05, BAI09.03, BAI03.10, BAI09.02, BAI09.03, DSS01.05	ISO A.11.2.7
12	FRM 12 - Form keluhan pelanggan	RS.CO-2, DE. DP-4, RS.CO-3	DSS01.03, APO08.04, APO12.06, DSS02.05, DSS03.04	ISO A.16.1.2, ISO 9001 tahun 2015
13	FRM 17 - Peminjaman Aset IT	PR.DS-5, PR.AC-4	APO01.06, DSS05.04, DSS05.07, DSS06.02	ISO A.9.1.1, ISO A.9.2
14	FRM 18 - User Data Recovery	PR.AC-2, PR.DS-3, PR.MA-1	DSS01.04, DSS05.05, BAI09.03, BAI03.10, BAI09.02, BAI09.03, DSS01.05	ISO A.11.2.7
15	FRM 19 - Daftar distribusi informasi	PR.AC-2, PR.DS-3, PR.MA-1	DSS01.04, DSS05.05, BAI09.03, BAI03.10, BAI09.02, BAI09.03, DSS01.05	ISO A.11.2.7
16	FRM 20 - Form stocktaking	PR.AC-2, PR.DS-3, PR.MA-1	DSS01.04, DSS05.05, BAI09.03, BAI03.10, BAI09.02, BAI09.03, DSS01.05	ISO A.11.2.7
17	FRM 21 - Form berita acara mutasi asset	PR.AC-2, PR.DS-3, PR.MA-1	DSS01.04, DSS05.05, BAI09.03, BAI03.10, BAI09.02, BAI09.03, DSS01.05	ISO A.11.2.7

No	Nama Dokumen	NIST	COBIT	ISO
18	FRM 22 - Daftar dokumen eksternal	PR. IP-4	APO13.01, DSS01.01, DSS04.07	ISO A.18.1.3
19	FRM 24 - Daftar dokumen backup	PR.AC-2, ID.AM-3, ID. GV-3, PR. IP-4	APO13.01, DSS01.04, DSS05.03, DSS05.02, BAI02.01, MEA03.01, MEA03.04, BAI01.06, BAI06.01	ISO A.11.2.7, ISO A.13.2.2, ISO A.18.1.3
20	FRM 25 - Review hak akses	PR.DS-5, PR.AC-4	APO01.06, DSS05.04, DSS05.07, DSS06.02	ISO A.9.1.1, ISO A.9.2
21	FRM 26 - Form review wrong access fisik	PR.DS-5, PR.AC-4	APO01.06, DSS05.04, DSS05.07, DSS06.02	ISO A.9.1.1, ISO A.9.2
22	FRM 27 - Log insiden	PR. IP-9, DE.AE-5, DE. DP-5, RS.CO-2, RS.MI-1	APO12.06, DSS04.03, APO12.06, DSS03.01, DSS04.05	ISO A.16
23	FRM 059 - Quality Assurance Aplikasi	PR.AC-3	DSS05.04, DSS06.03	ISO A.6.2.1
24	Nomor form	PR. IP-4	APO13.01, DSS01.01, DSS04.07	ISO A.18.1.3
25	FRM 28 - Log peminjaman aset IT	PR.AC-2, PR.DS-3, PR.MA-1	DSS01.04, DSS05.05, BAI09.03, BAI03.10, BAI09.02, BAI09.03, DSS01.05	ISO A.11.2.7
26	FRM 30 - Berita acara serah terima server	PR.DS-7	BAI03.08, BAI07.04	ISO A.12.1.4
27	FRM 31 - Perjanjian kerahasiaan employee	PR.AC-2, ID.AM-3, ID.GV-3, PR.IP-4	APO13.01, DSS01.04, DSS05.03, DSS05.02, BAI02.01, MEA03.01, MEA03.04, BAI01.06, BAI06.01	ISO A.11.2.7, ISO A.13.2.2, ISO A.18.1.3
28	FRM 32 - Form pernyataan menjaga kerahasiaan	PR.AC-2, ID.AM-3, ID.GV-3, PR.IP-4	APO13.01, DSS01.04, DSS05.03, DSS05.02, BAI02.01, MEA03.01, MEA03.04, BAI01.06, BAI06.01	ISO A.11.2.7, ISO A.13.2.2, ISO A.18.1.3
29	FRM 33 - Form kehilangan kartu	PR.AC-2, PR.DS-3, PR.MA-1	DSS01.04, DSS05.05, BAI09.03, BAI03.10, BAI09.02, BAI09.03, DSS01.05	ISO A.11.2.7
30	FRM 35 - Permohonan access card	PR.DS-5, PR.AC-4	APO01.06, DSS05.04, DSS05.07, DSS06.02	ISO A.9.1.1, ISO A.9.2
31	FRM 36 - FORM CAR	PR.DS-5	APO01.06, DSS05.04, DSS05.07, DSS06.02	ISO A.10.1

No	Nama Dokumen	NIST	COBIT	ISO
32	FRM 37 - Form pernyataan pertanggungjawab perangkat IT (HO)	PR.AC-1, PR.AC-2, PR.DS-3, PR.MA-1, PR.DS-7	DSS05.04, DSS06.03, DSS01.04, DSS05.05, BAI09.03, BAI03.10, BAI09.02, DSS01.05, BA107.04, BA.103.08	ISO A.9.3, ISO A.11.2.5 dan ISO A.12.1.4
33	FRM 38 - Form pernyataan pertanggungjawab perangkat IT (Cabang)	PR.AC-1, PR.AC-2, PR.DS-3, PR.MA-1, PR.DS-7	DSS05.04, DSS06.03, DSS01.04, DSS05.05, BAI09.03, BAI03.10, BAI09.02, DSS01.05, BA107.04, BA.103.08	ISO A.9.3, ISO A.11.2.5 dan ISO A.12.1.4
34	FRM 39 - Permintaan IT/IS Aplikasi	PR.AC-2, PR.DS-3, PR.MA-1	DSS01.04, DSS05.05, BAI09.03, BAI03.10, BAI09.02, BAI09.03, DSS01.05	ISO A.11.2.7
35	FRM 47 - Tracking form pengembangan aplikasi	PR.DS-5	APO01.06, DSS05.04, DSS05.07, DSS06.02	ISO A.6.1.2
36	FRM 48 - Surat permohonan penggunaan	PR.IP-1, ID.GV-3	BAI10.01, BAI10.02, BAI10.03, BAI10.05, BAI02.01, MEA03.01, MEA03.04	ISO A.12.6.2, ISO A.18.1.2
37	FRM 50 - Log perubahan dokumen	PR. IP-4	APO13.01, DSS01.01, DSS04.07	ISO A.18.1.3
38	FRM 53 - Bast Asset IT	PR.AC-2, PR.DS-3, PR.MA-1	DSS01.04, DSS05.05, BAI09.03, BAI03.10, BAI09.02, BAI09.03, DSS01.05	ISO A.11.2.7

3.2.2.2 Melakukan review dan improvement dokumen

Melakukan review mengenai dokumen kebijakan yang sesuai dengan standar internasional ISO 27001:2013. Jadi PT. United Tractors sudah mengimplementasikan menggunakan *framework* ISO 27001 untuk meningkatkan teknologi informasi dan keamanan. Namun, ada beberapa poin yang belum diimplementasikan oleh PT. United Tractors. Sehingga diperlukan improvement terhadap dokumen tersebut.

Table 3.5 Improvement Dokumen PLC dan SOP

No	Nama Dokumen	Rekomendasi yang diberikan kepada PT. United Tractors Tbk
1	PLC 02	Pengguna harus menggunakan perangkat lunak yang berlisensi dan sesuai dengan kebutuhan yang tepat.
2	PLC 03	PT. United Tractors tidak memperbolehkan untuk mengungkapkan informasi rahasia dengan keluarga, teman, atau membicarakannya di tempat umum.
		PT. United Tractors tidak memperbolehkan seluruh karyawan untuk mengungkapkan informasi di luar kewenangan yang dimilikinya, informasi yang salah, informasi yang tidak seluruhnya benar dan/atau informasi yang tidak lengkap.
		Sarana dalam penyampaian informasi sangat rahasia dan rahasia harus melalui sarana tertulis dan/atau lisan oleh direksi yang ditunjuk/berwenang.
		PT. United Tractors harus menyediakan informasi-informasi kepada publik berdasarkan klasifikasi informasi, kepentingan pihak yang membutuhkan, dan sesuai ketentuan perundang-undangan yang berlaku.
3	PLC 04	Seluruh wilayah terdapat CCTV dan *face acess door* agar dapat terjaga dengan aman.
4	PLC 05	Pengguna wajib menjaga kerahasiaan akses akun E-mail. Sehingga diperlukan adanya verifikasi akun sebelum masuk email.
		Apabila ada pengakhiran hubungan kerja antara karyawan dan perusahaan, maka perusahaan berhak untuk menutup E-mail karyawan dan penutupan akses terhadap seluruh sarana pesan elektronik.
		PT. United Tractors berhak untuk melakukan *blocking*, monitor, mengkaji, dan mengungkapkan setiap/semua pesan yang dikirimkan atau diterima.
5	PLC 06	Setiap karyawan yang memperoleh password wajib untuk menjaga kerahasiaan dan keamanan password.
		CST *Division* mempunyai kewenangan untuk menghapus/menonaktifkan seluruh *password* dari karyawan yang memiliki status mengundurkan diri atas permintaan dan pemberitahuan dari departemen HRD.
		Karyawan dilarang menggunakan *password* yang ada kaitannya dengan *username*, nama, alamat, nomor kartu identitas, nomor *telephone*, hari ulang tahun.
6	PLC 07	Divisi IT perlu melakukan pengecekan fisik perangkat IT dari hasil pengadaan barang maupun kerusakan barang secara berkala

No	Nama Dokumen	Rekomendasi yang diberikan kepada PT. United Tractors Tbk
7	PLC 08	Karyawan tidak diperbolehkan untuk melakukan *install software* perusahaan di PC/*Notebook* milik pribadi.
		Karyawan tidak diperbolehkan untuk menyalin program *software*.
8	PLC 10	Membuat *website* dengan menggunaan gambar, foto, desain, video orang lain.
		Setiap karyawan yang melanggar HAKI, maka akan mendapatkan sanksi/hukuman sesuai UUD
9	SOP 069	Dokumen yang mengalami perubahan harus diterbitkan kembali secara formal
10	SOP 070	Laporan audit internal ditandatangani oleh *lead auditor* sebelum diserahkan kepada *auditee* untuk kesepakatan terhadap ketidaksesuaiaan, penentuan tindakan koreksi dan pencegahan yang harus dilakukan oleh bagian yang bersangkutan.
11	SOP 071	Status tindakan dari tinjauan manajemen sebelumnya
		Perubahan atas isu eksternal dan internal yang relevan dengan *system* manajemen mutu.
13	SOP 072	Setelah mencatat, maka diperlukan adanya analisis ketidaksesuaian untuk menemukan akar penyebab terjadinya ketidaksesuaian tersebut.
14	SOP 073	Perlu adanya *service category*, *service type*, *service* status, *priority*, *service* review, dan *service availability* pada *service catalogue.*
15	SOP 079	Diperlukan melakukan pemeriksaan dan pengukuran hasil kerja sama dengan supplier.
		Diperlukan melakukan pembayaran, apabila ada kekurangan mengenai hasil pembelian atau kontrak dengan *supplier*.
		Melaporkan pengakhiran kontrak dalam bentuk laporan atau surat pemutusan kontrak.
16	SOP 081	Diperlukan adanya kategori insiden yang dibuat berdasarkan jenis insiden, perkiraan lamanya penaganan, impikasi insiden, dan waktu penutupan kasus. Tujuannya untuk menghasilkan kategori insiden dan prioritas penanganan yang sejalan dengan proses bisnis organisasi.
		Diperlukan adanya resolusi insiden yang bertujuan untuk menyelesaikan suatu insiden. Langkah resolusi dapat dilakukan oleh *service desk* sebagai pihak yang pertama menemukan insiden dari user, staf teknisi yang sedang

No	Nama Dokumen	Rekomendasi yang diberikan kepada PT. United Tractors Tbk
		mengerjakan kegiatan konfigurasi maupun oleh *supplier* terhadap perangkat yang masih dalam garansi.
17	SOP 085	Diperlukan adanya survei sistem *update software* untuk melihat ketahanan beberapa *software update system* terhadap *man-in-the middle attack*. (*Man in the middle attack* adalah salah satu jenis serangan siber yang dilakukan untuk mencuri data pengguna dengan menginterupsi komunikasi pengguna dengan *server*).
		Untuk mendukung *secure update* dapat menggunakan *secure notification*, dan merancang sistem yang aman
18	SOP 086	Membuat laporan catatan sebagai data mengenai perawatan, kegagalan, dan penggunaan setiap peralatan.
		Melakukan pemberhentian pemeliharaan apabila sedang menunjukkan gejala yang menyebabkan kerusakaan.

3.2.2.3 Membuat SOP terkait tanggap insiden keamanan

SOP insiden keamanan berisikan proses respons standar untuk keamanan siber dan menjelaskan proses proses dan penyelesaian melalui fase respons insiden. Prosedur ini berisikan langkah persiapan tanggap insiden, seperti kebijakan dan prosedur, peralatan, latih personal respons, kecerdasan ancaman siber, pertahanan aktif, komunikasi dan logistic, OPSEC, infrastruktur teknis, dan mendeteksi aktivitas.

3. PENGERTIAN ISTILAH

3.1. Manajemen CST adalah para pihak pengambil keputusan terkait layanan yaitu department head dan division head di Corporate Strategic & Technology Division.

3.2. Kerentanan adalah setiap atribut perangkat keras, perangkat lunak, pross, atau prosedur yang dapat mengaktifkan atau memfasilitasi kekalahan control keamanan.

4. REFERENSI

4.1. ISO/IEC 27002:2013 – 16.1.1 Responsibilities and procedures

4.2. ISO/IEC 27002:2013 – 16.1.3 Reporting information security weaknesses

5. KETENTUAN

5.1. Langkah Persiapan Tanggap Insiden

5.1.1. Kebijakan dan Prosedur

A. Dokumentasikan rencana Tanggap Insiden agensi dengan prosedur untuk meningkatkan dan melaporkan insiden besar dan insiden yang berdampak pada misi agensi.

B. Prosedur dokumen untuk menunjuk pimpinan koordinasi insiden lembaga.

C. Mengidentifikasi personel dan tanggung jawab tanggap insiden utama. Berikan nama POC, nomor telepon, dan alamat email

D. Identifikasi pemilik sistem dan petugas keamanan sistem informasi

E. Identifikasi IP Sistem, rencana keamanan sistem, batas sistem, status esensial misi dll

F. Dokumentasikan rencana darurat untuk sumber daya tambahan dengan peran dan tanggung jawab yang ditetapkan

5.1.2. Peralatan

A. Terapkan kemampuan deteksi dan pemantauan untuk menyertakan AV, EDR, DLP, IDPS, log, arus bersih, PCAP, dan

SIEM untuk memberikan gambaran yang akurat tentang infrastruktur agensi (sistem, jaringan, platform cloud, dan jaringan yang dihosting oleh kontraktor).

B. Tetapkan garis dasar untuk sistem dan jaringan untuk memahami aktivitas "normal" apa yang memungkinkan pembela HAM mengidentifikasi setiap penyimpangan.

C. Menerapkan kemampuan EINSTEIN.

D. Menerapkan kemampuan CDM.

E. Pastikan logging, penyimpanan log, dan manajemen log mematuhi EO 14028, Sec 8

5.1.3. Latih Personel Respons

A. Latih dan olah badan dan personel kepegawaian untuk bersiap menghadapi insiden besar.

B. Lakukan latihan pemulihan untuk menguji COOP organisasi penuh (failover/ backup/recovery systems).

5.1.4. Kecerdasan Ancaman Siber

A. Pantau umpan intelijen untuk saran ancaman atau kerentanan dari berbagai sumber: pemerintah, mitra tepercaya, sumber terbuka, dan entitas komersial

B. Integrasikan umpan ancaman ke dalam SIEM dan kemampuan pertahanan lainnya untuk mengidentifikasi dan memblokir perilaku jahat yang diketahui

C. Menganalisis laporan aktivitas mencurigakan dari pengguna, kontraktor/ penyedia layanan TIK; atau laporan insiden dari komponen organisasi internal atau eksternal lainnya.

D. Kumpulkan data insiden (indikator, TTP, penanggulangan) dan bagikan dengan CISA dan mitra lainnya (penegak hukum, dll.)

E. Siapkan CISA Automated Indicator Sharing (AIS) atau bagikan melalui Cyber Threat Indicator dan Defensive Measures Submission System.

5.1.5. Pertahanan Aktif

Bagi mereka yang memiliki kemampuan dan staf tingkat lanjut, bangun mekanisme pertahanan aktif (yaitu, honeypots, honeynets, honeytoken, akun palsu, dll.) untuk membuat kabel trip untuk mendeteksi penyusupan musuh dan mempelajari perilaku musuh untuk lebih memahami TTP mereka.

5.1.6. Komunikasi dan logistic

A. Menetapkan strategi komunikasi. Ini termasuk: Menentukan protokol komunikasi email out-of-band, Menetapkan ruang perang, Menetapkan saluran komunikasi (jembatan telepon atau ruang obrolan)

B. Menetapkan mekanisme prosedur untuk mengkoordinasikan insiden besar dengan CISA.

C. Tunjuk POC pelaporan CISA. Berikan nama POC, nomor telepon, dan alamat email. Terapkan format dan platform berbagi info ke CISA

D. Tentukan metode untuk menyerahkan informasi dan data rahasia, jika diperlukan.

5.1.7. OPSEC

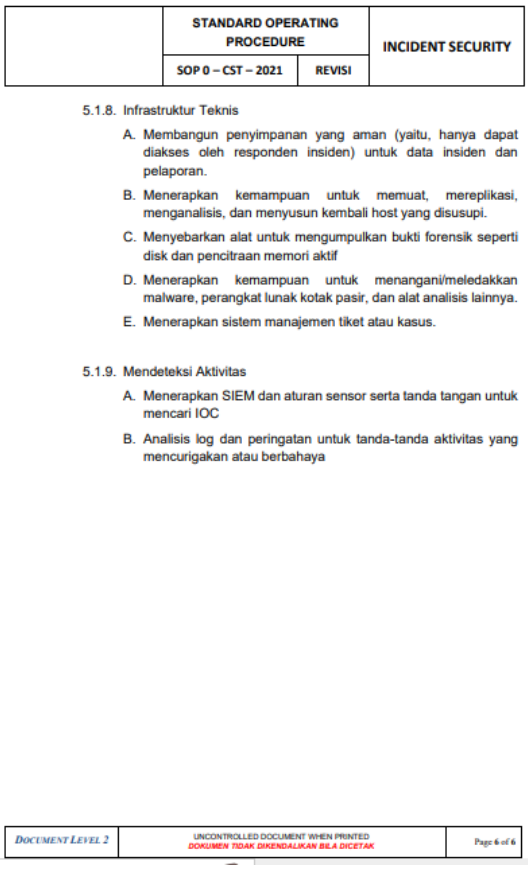
A. Segmentasikan/kelola sistem SOC secara terpisah dari sistem TI perusahaan yang lebih luas. Kelola sensor dan perangkat keamanan melalui sarana out-ofband (jaringan, dll).

B. Kembangkan metode untuk memberi tahu pengguna tentang sistem yang dikompromikan melalui telepon daripada email.

C. Gunakan stasiun kerja yang diperkeras untuk melakukan aktivitas pemantauan dan respons.

D. Pastikan sistem pertahanan memiliki proses pencadangan dan pemulihan yang kuat.

E. Terapkan proses untuk menghindari "membocorkan" penyerang untuk mengurangi kemungkinan deteksi informasi sensitif IR (misalnya, jangan mengirim sampel malware ke layanan analisis publik atau memberi tahu pengguna tentang sistem yang disusupi melalui email).



	STANDARD OPERATING PROCEDURE		INCIDENT SECURITY
	SOP 0 – CST – 2021	REVISI	

5.1.8. Infrastruktur Teknis

A. Membangun penyimpanan yang aman (yaitu, hanya dapat diakses oleh responden insiden) untuk data insiden dan pelaporan.

B. Menerapkan kemampuan untuk memuat, mereplikasi, menganalisis, dan menyusun kembali host yang disusupi.

C. Menyebarkan alat untuk mengumpulkan bukti forensik seperti disk dan pencitraan memori aktif

D. Menerapkan kemampuan untuk menangani/meledakkan malware, perangkat lunak kotak pasir, dan alat analisis lainnya.

E. Menerapkan sistem manajemen tiket atau kasus.

5.1.9. Mendeteksi Aktivitas

A. Menerapkan SIEM dan aturan sensor serta tanda tangan untuk mencari IOC

B. Analisis log dan peringatan untuk tanda-tanda aktivitas yang mencurigakan atau berbahaya

DOCUMENT LEVEL 2	UNCONTROLLED DOCUMENT WHEN PRINTED DOKUMEN TIDAK DIKENDALIKAN BILA DICETAK	Page 6 of 6

3.2.2.4 Mempelajari dokumen kebijakan, SOP, IK, dan Form

Terdapat beberapa dokumen milik PT. United Tractors Tbk yang sudah sesuai dengan standar ISO 27001:2013. Dokumen tersebut yaitu dokumen kebijakan, SOP, IK, dan Form yang sesuai dengan standar ISO 27001:2013 yang terdiri dari klausa-klausa ISO 27001:2013. Berikut adalah penjelasan dari setiap dokumenya yaitu:

1) Kebijakan/*Policy* adalah serangkaian kegiatan atau konsep yang dapat menjadi suatu pedoman dalam melaksanakan pekerjaan seperti tujuan, cara bertindak dll.
2) SOP adalah prosedur yang digunakan untuk memastikan bahwa kegiatan operasional organisasi atau perusahaan dapat berjalan sesuai dengan prosedur.

3) Form adalah dokumen yang berisikan data-data dalam pelaksanaan proses perusahaan.
4) IK adalah tahapan dalam melaksanakan setiap kegiatan dalam suatu proses.

3.2.2.5 Membuat infografis terkait awareness ISO 27001

Pembuatan infografis ini akan ditujukan ke seluruh karyawan PT. United Tractors Tbk. Pembuatan infografis ini bertujuan untuk memperkenalkan dan meningkatkan kepeduliaan karyawan terhadap keamanan informasi yang sesuai dengan ISO 27001:2013. Beberapa infografis ini berisikan tentang contoh implementasi ISO 27001:2013. Pembuatan infografis ini dikerjakan menggunakan *website* Canva yang diperlukan untuk membuat design, lalu melakukan pengisian informasi atau konten infografis. Berikut beberapa infografis yang dapat meningkatkan kepedulian karyawan terhadap keamanan informasi yang sesuai dengan ISO 27001:2013 sebagai berikut

1) Infografis terkait cara mencegah overheating laptop.

Gambar 3.1 Infografis Overheating Laptop

Pada gambar 3.1 berisikan infografis terkait cara mencegah overheating laptop yang dimana ini adalah contoh implementasi pada ISO 27001:2013 klausa A.11.1 *Physical and Environmental Security* (Keamanan Fisik dan Lingkungan) untuk mencegah kerusakan pada aset fisik. Sehingga diperlukan control untuk menjaga seluruh fasilitas atau peralatan milik perusahaan.

2) Infografis terkait amankah komputer anda.

Gambar 3.2 Infografis Amankah Komputer Anda

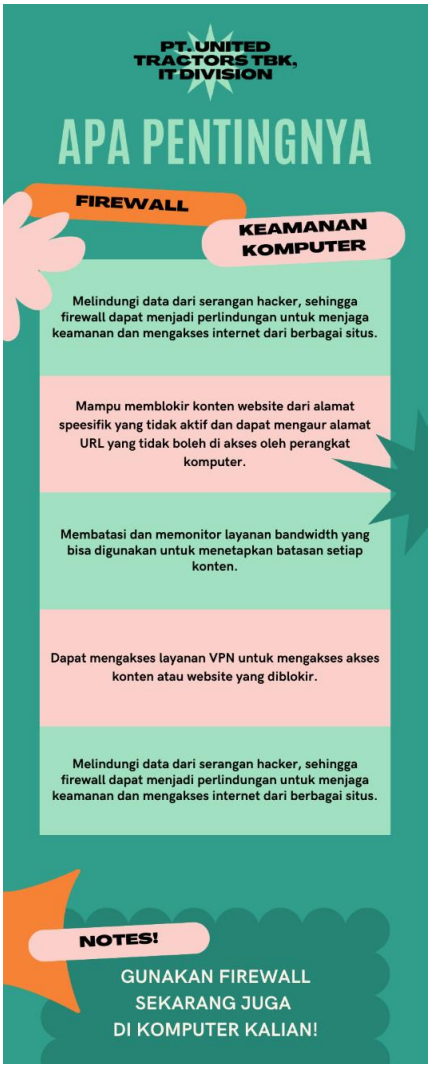
Pada gambar 3.2 berisikan infografis terkait amankah komputer anda yang dimana ini adalah contoh implementasi pada ISO 27001:2013 klausa A.12 *Operations Security* (Keamanan Operasi) untuk memastikan fasilitas atau peralatan pemrosesan informasi dapat berjalan dengan baik dan aman. Sehingga diperlukan control untuk melindungi komputer dengan antivirus, *update windows*, *back-up* berkas dll.

3) Infografis terkait tips karyawan menjaga *cyber security* saat bekerja.

Gambar 3.3 Tips Menjaga Cyber Security

Pada gambar 3. 3 berisikan infografis tips karyawan menjaga *cyber security* saat bekerja yang dimana ini adalah contoh implementasi pada ISO 27001:2013 klausa A.6 *Organization of Information Security* (Keamanan Informasi Perusahaan) untuk memastikan sumber daya dapat menerapkan dan memelihara keamanan informasi secara memadai. Sehingga diperlukan *control* untuk melindungi data menggunakan *password*, *multifactor* autentikasi, menggunakan VPN dll.

4) Infografis terkait apa pentingnya firewall.



Gambar 3.4 Infografis Pentingnya Firewall

Pada gambar 3.4 berisikan infografis terkait apa pentingnya *firewall* yang dimana ini adalah contoh implementasi pada ISO 27001:2013 klausa A.11 *Physical and Environmental Security (Keamanan Fisik dan Lingkungan)* untuk mencegah kerusakan informasi atau komputer. Sehingga diperlukan control untuk menjaga keamanan komputer menggunakan *firewall*.

5) Infografis terkait langkah-langkah yang bisa dilakukan untuk *cyber-attacks*.

Gambar 3.5 Infografis Cyber Attacks

Pada gambar 3.5 berisikan infografis terkait langkah-langkah yang bisa dilakukan untuk *cyber-attacks* yang dimana ini adalah contoh implementasi pada ISO 27001:2013 klausa A.12 *Operations Security* (Keamanan Operasi) untuk memastikan fasilitas atau peralatan pemrosesan informasi dapat berjalan dengan baik dan aman. Sehingga diperlukan *control* untuk melindungi komputer dengan *antivirus*, *update windows*, *back-up* berkas dll.

6) Infografis contoh *operation security* pada ISO 27001.

Gambar 3.6 Infografis Operation Security

Pada gambar 3.6 berisikan infografis terkait amankah komputer anda yang dimana ini adalah *contoh operations security* pada ISO 27001 ISO 27001:2013 klausa A.12 *Operations Security* (Keamanan Operasi) untuk memastikan

fasilitas atau peralatan pemrosesan informasi dapat berjalan dengan baik dan aman. Sehingga diperlukan control untuk melindungi kegiatan operasi dll.

7) Infografis terkait kebijakan *clear desk* dan *clear screen* ISO 27001

Gambar 3.7 Infografis Clear Desk dan Clear Screen

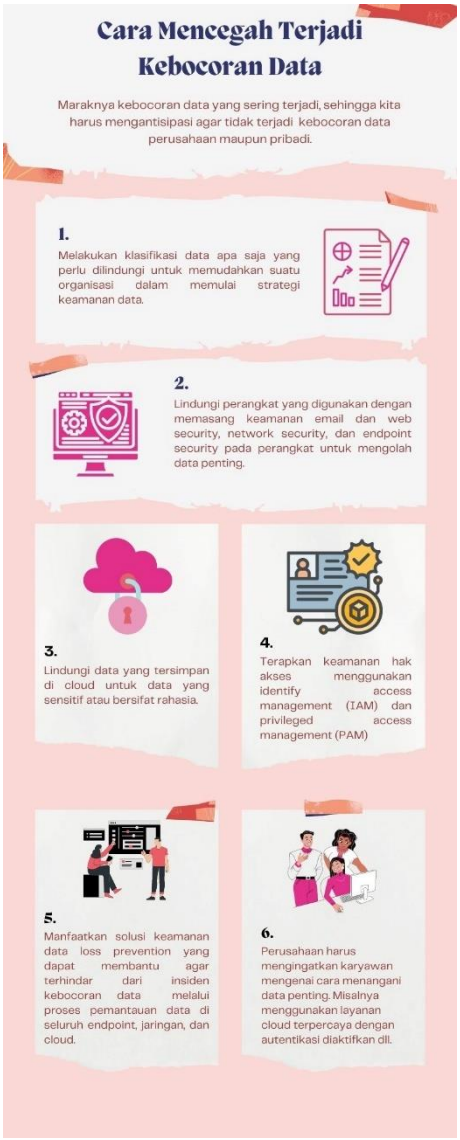
Pada gambar 3.7 berisikan infografis terkait kebijakan *clear desk* dan *clear screen* yang dimana ini adalah contoh implementasi pada ISO 27001:2013 klausa A.11.1 *Physical and Environmental Security* (Keamanan Fisik dan Lingkungan) untuk mencegah kehilangan, kerusakan atau pencurian peralatan aset informasi. Sehingga diperlukan control untuk menjaga lokasi lingkungan perusahaan, menjaga keamanan peralatan yang pelihara dll.

8) Infografis terkait cara mengatasi kebocoran data.

Gambar 3.8 Infografis Kebocoran Data

Pada gambar 3.8 berisikan infografis terkait cara mengatasi terjadi kebocoran data yang dimana ini adalah contoh implementasi pada ISO 27001:2013 klausa A.6 *Organisation of Information Security (Keamanan Informasi Perusahaan)* untuk menerapkan dan memelihara keamanan informasi secara memadai. Sehingga diperlukan untuk melindungi data, selalu *update software* dll.

9) Infografis terkait cara mencegah terjadi kebocoran data.



Gambar 3.9 Infografis Cara Mencegah Kebocoran Data

Pada gambar 3.9 berisikan infografis terkait cara mencegah kebocoran data yang dimana ini adalah contoh implementasi pada ISO 27001:2013 klausa A.6 *Organisation of Information Security (Keamanan Informasi Perusahaan)* untuk memastikan fasilitas atau peralatan pemrosesan informasi dapat berjalan dengan baik dan aman. Sehingga diperlukan *control* untuk menerapkan dan memelihara keamanan informasi secara memadai. Sehingga diperlukan untuk melindungi data, selalu *update software* dll.

10) Infografis terkait menjaga data pribadi di laptop.

Gambar 3.10 Infografis Menjaga Data Pribadi

Pada gambar 3.10 berisikan infografis terkait cara menjaga data pribadi yang dimana ini adalah contoh implementasi pada ISO 27001:2013 klausa A.11 *Physical and Environmental Security* (Keamanan Fisik dan Lingkungan) untuk mencegah kehilangan, kerusakan, dan pencurian peralatan aset informasi perusahaan. Sehingga diperlukan control dalam menggunakan *password*, menggunakan VPN dll.

11) Infografis terkait cara menghindari *malware.*

Gambar 3.11 Infografis Cara Menghindari Malware

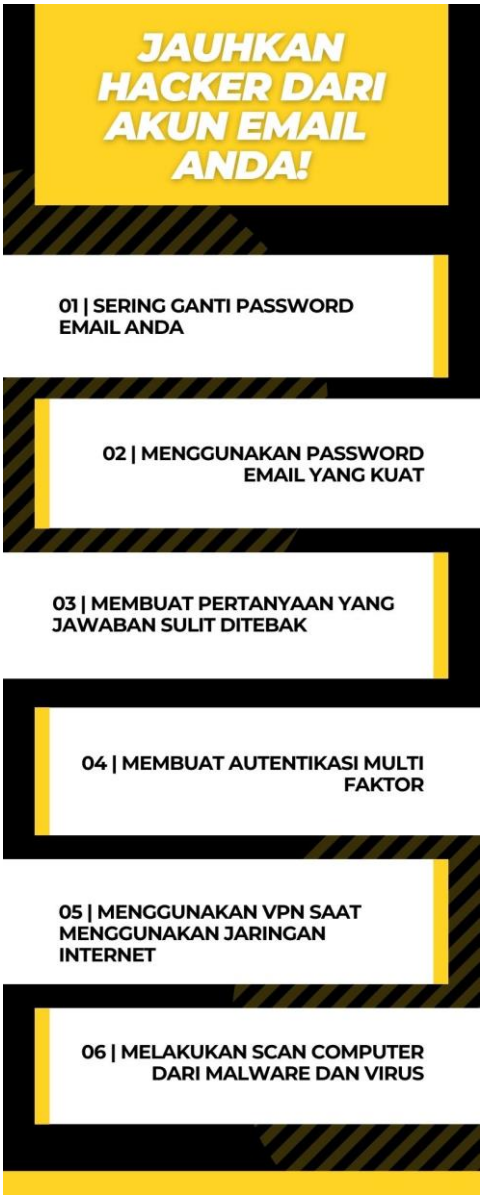
Pada gambar 3.11 berisikan infografis terkait amankah komputer anda yang dimana ini adalah contoh implementasi pada ISO 27001:2013 klausa A.12 *Operations Security* (Keamanan Operasi) untuk memastikan fasilitas atau peralatan pemrosesan informasi dapat berjalan dengan baik dan aman. Sehingga diperlukan control untuk melindungi komputer dengan antivirus, *update windows*, *back-up* berkas dll.

12) Infografis terkait *how strong are your passwords.*

Gambar 3.12 Infografis How Strong Are Your Passwords

Pada gambar 3.12 berisikan infografis terkait *how strong your password* yang dimana ini adalah contoh implementasi pada ISO 27001:2013 klausa A.11 *Physical and Environmental Security* (Keamanan Fisik dan Lingkungan) untuk menjaga keamanan informasi atau data perusahaan dengan menggunakan *password* yang unik dan kuat.

13) Infografis terkait jauhkan hacker dari akun *E-mail* anda.



Gambar 3.13 Infografis Jauhkan Hacker dari E-mail

Pada gambar. 3.13 berisikan infografis terkait jauhkan hacker dari akun email anda yang dimana ini adalah contoh implementasi pada ISO 27001:2013 klausa A.6 *Organisation of Information Security* (Keamanan Informasi Perusahaan) untuk bertanggung jawab dalam menjaga keamanan *E-mail* perusahaan. Sehingga diperlukan *control* dalam menggunakan *password* yang unik atau kuat, melakukan *scan computer* dari *malware* dan virus dll.

14) Infografis terkait tips menghindari serangan *phising*.

Gambar 3.14 Infografis Phising

Pada gambar 3.14 berisikan infografis terkait tips menghindari serangan *phising* yang dimana ini adalah contoh implementasi pada ISO 27001:2013 klausa A.6 *Organisation of Information Security (Keamanan Informasi Perusahaan)* untuk memberikan perlindungan informasi. Sehingga diperlukan control untuk menjaga keamanan informasi.

15) Infografis terkait waspada bahaya *software* bajakan

Gambar 3.15 Infografis Waspada Software Bajakan

Pada gambar 3.15 berisikan infografis terkait waspada *software* bajakan yang dimana ini adalah contoh implementasi pada ISO 27001:2013 klausa A.18 *Compliance* (Kepatuhan) untuk mencegah terjadinya penggunaan *software* bajakan. Sehingga diperlukan control untuk menggunakan *software* yang resmi.

16) Infografis terkait cara merawat *software* komputer anda

Gambar 3.16 Infografis Merawat Software Komputer

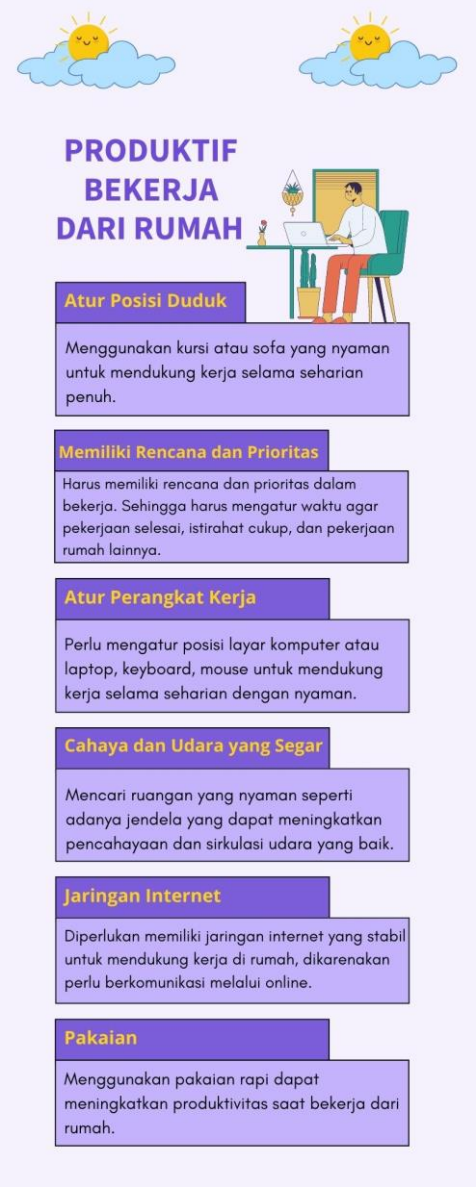
Pada gambar 3.16 berisikan infografis terkait cara merawat software komputer anda yang dimana ini adalah contoh implementasi pada ISO 27001:2013 klausa A.18 *Compliance* (Kepatuhan) untuk mencegah masuknya virus sehingga diperlukan menggunakan software yang legal.

17) Infografis terkait cara membersihkan layar monitor laptop

Gambar 3.17 Infografis Cara Membersihkan Layar Monitor

Pada gambar 3.17 berisikan infografis terkait cara membersihkan layar monitor yang dimana ini adalah contoh implementasi pada ISO 27001:2013 klausa A.11 *Physical and Environmental Security* (Keamanan Fisik dan Lingkungan) untuk memastikan peralatan atau fasilitas yang diberikan terjaga dan terpelihara dengan baik. Sehingga diperlukan membersihkan layar monitor dengan rutin.

18) Infografis Produktif Bekerja dari Rumah



Gambar 3.18 Infografis Produktif Bekerja Dari Rumah

Pada gambar 3.18 berisikan infografis terkait produktif bekerja dari rumah yang dimana ini adalah contoh implementasi pada ISO 27001:2013 klausa A.6 *Organisations of Information Security (Keamanan Informasi Perusahaan)* untuk dapat menerapkan dan memelihara keamanan informasi secara memadai. Sehingga diperlukan dalam menerapkan cara produktif bekerja dari rumah.

19) Infografis Jaga Keamanan Jejak Digital

Gambar 3.19 Infografis Jaga Keamanan Jejak Digital

Pada gambar 3.19 berisikan infografis terkait jaga keamanan jejak digital yang dimana ini adalah contoh implementasi pada ISO 27001:2013 klausa A.11 *Physical and Environmental Security (Keamanan Fisik dan Lingkungan)* untuk mencegah kehilangan atau pencurian aset informasi. Sehingga diperlukan control untuk menjaga keamanan jejak digital.

20) Infografis terkait cara membersihkan keyboard dengan baik

Gambar 3.20 Infografis Cara Membersihkan Keyboard dengan Baik

Pada gambar 3.20 berisikan infografis terkait cara membersihkan keyboard dengan baik yang dimana ini adalah contoh implementasi pada ISO 27001:2013 klausa A.11 *Physical and Environmental Security* (Keamanan Fisik dan Lingkungan) untuk memastikan fasilitas atau peralatan dapat terpelihara dengan baik. Sehingga diperlukan control untuk membersihkan keyboard secara rutin.

21) Infografis terkait tips aman menggunakan *WIFI public* atau umum

Gambar 3.21 Infografis Tips Aman Menggunakan WIFI

Pada gambar 3.21 berisikan infografis terkait tips menggunakan *WIFI public* atau umum yang dimana ini adalah contoh implementasi pada ISO 27001:2013 klausa A.11 *Physical and Environmental Security* (Keamanan Fisik dan Lingkungan) untuk menghindari masuknya *hacker* kedalam komputer. Sehingga diperlukan dalam menjaga keamanan dalam menggunakan wifi umum.

22) Infografis terkait cara ampuh meningkatkan keamanan jaringan

Gambar 3.22 Infografis Cara Meningkatkan Keamanan Jaringan

Pada gambar 3.22 berisikan infografis terkait cara ampuh meningkatkan keamanan jaringan yang dimana ini adalah contoh implementasi pada ISO 27001:2013 klausa A.13 *Communiction Security* (Keamanan Informasi) untuk menjaga keamanan jaringan di seluruh perangkat jaringan. Sehingga diperlukan control untuk mengatur dan melakukan konfigurasi perangkat jaringan, monitoring jaringan dll.

23) Infografis terkait perbedaan ISO 27001 dan ISO 20000

Gambar 3.23 Infografis Perbedaan ISO 27001 dan 20000

Pada gambar 2.23 ini infografis terkait perbedaan ISO 27001 dan 20000 yang dimana terdapat 5 perbedaan seperti, ISO 27001 berbasis manajemen risiko sedangkan ISO 20000 berbasis layanan dan menggap risiko sebagai elemen bangunan.

24) Infografis terkait manfaat ISO 27001

Gambar 3.24 Infografis Manfaat ISO 20000

Pada gambar 3.24 infografis ini terkait manfaat ISO 20000 yang dimana membahas dari 5 bagian yaitu kepuasan pelanggan, daya saing dan kredibilitas, tolak ukur dan perbadikan, kepatuhan, dan produktivitas.

25) Infografis terkait prinsip standar ISO 27001

Gambar 3.25 Infografis Prinsip Standar ISO 27001

Pada gambar 3.25 ini berisikan infografis terkait prinsip standar ISO 27001 yang dimana *Plan-Do-Check-Act.* Untuk *Plan* yaitu merencanakan, *Do* yaitu menerapkan, *Check* yaitu memantau, dan *Act* yaitu mengambil tindakan.

26) Infografis terkait keuntungan sertifikasi ISO 27001

Gambar 3.26 Infografis Keuntungan Sertifikasi ISO 27001

Pada gambar 3.26 infografis ini berisikan keuntungan mengikuti sertifikasi ISO 27001 yang dimana beberapa perusahaan sudah menerapkan ISO 27001 karena dapat meningkatkan kepercayaan pelanggan dll.

3.2.2.6 Mempelajari dan membuat materi ISO 27001:2022, ISO 27701:2019 dan CAASM dalam bentuk PPT.

1) CAASM *(Cyber Security Asset Security Management)*

Pembuatan materi presentasi terkait CAASM ini dilakukan pada minggu keenambelas. CAASM adalah sebuah teknologi baru yang berfokus pada tim keamanan untuk memecahkan masalah yang tetap dengan visibilitas aset dan kerentanan tantangan. Materi presentasi ini berisikan sejarah dari CAASM, pengertian dari CAASM dll.

2) ISO 27701:2019 (Sistem Informasi Manajemen Data Pribadi)

   Pembuatan materi terkait ISO 27701:2019 (Sistem Informasi Manajemen Data Pribadi) ini dilakukan pada minggu keenambelas. ISO 27701:2019 ini merupakan lanjutan dari ISO 27001 yang menerapkan sertifikasi ISO 27701. ISO 27701 ini memandu organisasi tentang kebijakan dan prosedur untuk mematuhi peraturan dan undang-undang perlindungan/privasi.

3) ISO 27001:2022

   Pembuatan materi terkait ISO 27001:2022 (Sistem Informasi Manajemen Data Pribadi) ini dilakukan pada minggu keenambelas. ISO 27001 akan diperbarui setiap 5 tahun, sehingga hal ini untuk menjaga standar manajemen informasi. PPT ini membahas terkait mengapa ISO 27001 diperbarui, perubahan apa yang diharapkan dengan ISO 27001:2022, kapan ISO 27001:2022 mulai berlaku dll.

3.2.2.7 Mengerjakan impovement dokumen Kebijakan (PLC) sesuai standar internasional COBIT

Table 3.6 Pemetaan Dokumen PLC sesuai Framework COBIT

No	Nama Dokumen	Kondisi Awal	Rekomendasi	Target
1	PLC 001 - Kebijakan Keamanan Teknologi Informasi	Terdapat dokumen kebijakan keamanan IT, namun belum tersedia dokumen kebijakan *business case*.	Untuk mendukung strategi bisnis juga diperlukan membuat dokumen kebijakan studi kasus bisnis (*business case*) yang bertujuan untuk melihat bagaimana solusi IT dapat menghasilkan nilai bisnis. Sehingga perlu ditambahkan dokumen *business case*.	Perlu adanya dokumen kebijakan *business case* sebagai panduan dalam karyawan bertanggung jawab menjaga keamanan informasi.
2		Mendeskripsikan mengenai bagaimana pengawasan keamanan IT di PT. United Tractors Tbk.	PT. United Tractors diperlukan melakukan audit manajemen keamanan informasi secara terperinci dengan menggunakan standar internasional/nasional yang berlaku. Sehingga dapat terlihat apakah keamanan IT di lingkungan PT. United Tractors sudah berjalan sesuai prosedur atau tidak?	Perlu dilakukan audit manajemen keamanan informasi.
3		Mendeskripsikan mengenai tanggung jawab personil dalam pengamanan informasi dalam pekerjaan sehari-hari	Meningkatkan pengetahuan keamanan informasi pada seluruh lingkungan divisi PT. United Tractors untuk meningkatkan pemahaman pengguna mengenai keamanan informasi.	Perlu adanya webinar/seminar dan poster mengenai pengetahuan keamanan informasi.
4		Mengenai perencanaan keamanan IT yang jelas, realistis, dan didokumentasikan kepada pemenuhan kebutuhan informasi.	PT. United Tractors membuat dokumen tentang rekomendasi untuk meningkatkan Sistem Manajemen Keamanan Informasi.	Perlu adanya dokumen rekomendasi SMKI

No	Nama Dokumen	Kondisi Awal	Rekomendasi	Target
5		Tidak adanya dokumen kebijakan pemantauan dan pelaporan manajemen keamanan informasi	Melengkapi Dokumen Tata Kelola TI dengan menambahkan kebijakan untuk melakukan pemantauan dan pelaporan terkait proses manajemen keamanan informasi yang dijalankan.	Perlu adanya dokumen kebijakan pemantauan dan pelaporan SMKI
6		Belum adanya pemantauan infrastruktur secara detail pada setiap hal yang terkait keamanan informasi yang dapat berpengaruh pada bisnis perusahaan.	Dilakukan pemantauan infrastruktur IT secara detail	Selain adanya CCTV dan *access door* di setiap ruangan, diperlukan juga pendefinisan karakteristik risiko keamanan informasi untuk mencatat risiko-risiko infrastruktur IT seperti kegagalan jaringan, keruskaan *hardware* dan *software*, kehilangan data dll.
7		Belum adanya pengujian keamanan informasi pada sistem informasi yang diimplementasikan.	Dilakukan pengujian keamanan informasi pada sistem informasi yang diimplementasikan dengan cara *penetration test* dan *vulnerability assessment*.	Perlu dilakukan *penetration test* dan *vulnerability assessment*.
8		Belum adanya dokumen yang mendefinisikan, mengatur, dan memberikan pedoman kegiatan dalam prosedur perlindungan sistem informasi dan teknologi dari *malware* sebagai prinsip dasar kegiatan perlindungan dari *malware*. Hanya terdapat pencatatan insiden, definisi, dan contoh *malware* yang terdapat pada PLC 01 dan SOP 088.	Adanya dokumen kebijakan pencegahan perangkat lunak berbahaya sebagai prinsip dasar kegiatan perlindungan dari *malware*.	Perlu adanya dokumen mengenai cara pencegahan perangkat lunak berbahaya dari *malware.*

No	Nama Dokumen	Kondisi Awal	Rekomendasi	Target
9		Belum adanya *webinar* atau infografis poster atau pelatihan mengenai informasi perlindungan perangkat lunak dari *malware.*	Perlu adanya webinar atau infografis poster atau pelatihan tentang perlindungan perangkat lunak dari *malware.*	Perlu adanya pelatihan melalui *webinar* atau infografis poster menganai perlindungan perangkat lunak dari *malware*.
10	PLC 002 - Kebijakan Penggunaan Aset IT Pribadi	Tidak adanya dokumen terkait perjanjian pemeliharaan aset IT.	Membuat dokumen terkait perjanjian pemeliharaan aset IT.	Adanya dokumen perjanjian pemeliharaan aset IT.
11	PLC 003 - Kebijakan Klasifikasi Informasi	Belum adanya dokumen mengenai evaluasi ancaman potensial yang akan terjadi pada keamanan informasi di perusahaan.	Perlu adanya dokumen evaluasi ancaman potensial keamanan informasi yang berisikan daftar potensi ancaman terhadap keamanan informasi yang dapat terjadi di perusahaan.	Perlu adanya dokumen potensial keamanan.
12		Belum adanya pengelolaan dokumen penting dan perangkat *output*.	Perlu adanya pengelolaan dokumen penting dan perangkat *output.*	Adanya pengelolaan dokumen dan perangkat *output* (laptop, printer, dan sejenisnya).
13		Belum ada kebijakan tentang menentukan otorisasi terhadap *devices* yang boleh mengakses informasi institusi dan jaringan insitusi.	Dibuatkan kebijakan untuk menentukan otorisasi terhadap *devices* yang boleh mengakses informasi dan jaringan perusahaan.	Adanya kebijakan otorisasi *devices* yang dapat mengakses informasi dan jaringan.
14		Belum adanya kebijakan untuk keamanan konektivitas berdasarkan penilaian risiko.	Dibuatkan kebijakan untuk keamanan konektivitas berdasarkan penilaian risiko kemudian dianalisis.	Adanya kebijakan keamanan konektivitas penilaian risiko.

No	Nama Dokumen	Kondisi Awal	Rekomendasi	Target
15	PLC 005 - Kebijakan Penggunaan Email dan Internet	Kurang melakukan sosialisasi berkala tentang penggunaan internet dan *Email*.	Melakukan sosialisasi berkala tentang penggunaan internet dan *Email*.	Adanya sosialisasi berkala tentang penggunaan internet dan *Email* melalui seminar/infografis agar karyawan mengetahui tentang penggunaan yang baik dilakukan dalam menggunakan internet dan *Email*. Mungkin bisa dilakukan juga untuk karyawan baru, akan diberikan 1 koordinator/penanggung jawab yang akan mengajarkan cara menggunakan *Email* perusahaan.
16		Kurang adanya informasi mengenai cara pencegahan kejahatan email seperti *spamming*, *scannng*, *phishing*, *malware*.	Adanya informasi mengenai cara pencegahan kejahatan *Email* yang sering terjadi di perusahaan.	Dapat dilakukan melalui infografis atau seminar mengenai cara pencegahan agar tidak terjadi kejahatan *Email* sehingga akan menambah wawasan karyawan dan *awareness* terhadap penggunaan *Email*.
17	PLC 006 - Kebijakan Manajemen *Password*	Akun-akun yang harus terlindungi dengan pengaturan pengelolaan hak akses sesuai dengan kewenangan pegawai.	Setiap karyawan yang memperoleh *password* wajib untuk menjaga kerahasiaan dan keamanan *password*.	Perlu adanya kebijakan khusus mengenai data *privacy*.
18	PLC 007 - Kebijakan pengelolaan *computer*, *printer*, dan *handheld device*	Belum adanya analisis perangkat IT secara rutin untuk mencegah ancaman yang timbul dari tindakan manusia seperti pencurian, dan juga terlindung dari ancaman lain seperti kebocoran data, hujan, bahaya kebakaran dll.	Perlu adanya analisis perangkat IT secara rutin untuk mencegah adanya ancaman yang timbul	Perlu adanya analisis perangkat IT secara rutin

3.2.2.8 Mempelajari dan mengerjakan risk assessment

Risk assessment adalah aktivitas yang dilaksanakan untuk memperkirakan suatu risiko dari situasi yang bisa didefinisikan dengan jelas atau potensi dari suatu ancaman atau bahaya baik

secara kuantitatif atau kualitatif. Sebelum dilakukannya rincian rencana pengendalian seperti kebutuhan dokumen, teknologi dan penunjang. Maka diperlukan adanya identifikasi risiko (klasifikasi aset, ancaman, kerawanan, potensi risiko), dilakukan penilaian risiko bawaan (inherent risiko), penilaian residual risiko, score nilai, dan control yang ada saat ini. Lalu yang terakhir memberikan rekomendasi rincian rencana pengendalian.

Berikut hasil pengerjaan magang saya mengenai rincian rencana pengendalian :

1) Risk Assessment Informasi

   Berikut table 3.7 *risk assessment* terkait informasi yang berisikan rincian rencana pengendalian, seperti kebutuhan dokumen, kebutuhan teknologi, dan kebutuhan penunjang.

Table 3.7 Risk Assessment Informasi

Risk No	**Rincian Rencana Pengendalian**		
	Kebutuhan Dokumen	**Kebutuhan Teknologi**	**Kebutuhan Penunjang**
INF-01	Dokumen kebijakan terkait sistem keamanan informasi.	Menerapkan standar privasi dan keamanan untuk mengakses informasi tersebut, menggunakan password dll.	Adanya sosialisasi mengenai keamanan informasi data.
INF-02	Dokumen kebijakan terkait sistem keamanan informasi.	-	Adanya sosialisasi mengenai keamanan informasi data.
INF-03	Dokumen kebijakan terkait sistem keamanan informasi.	Menerapkan standar privasi dan keamanan untuk mengakses informasi tersebut, menggunakan *password* dll.	Adanya sosialisasi mengenai keamanan informasi data.
INF-05	Adanya dokumen kerahasiaan perusahaan.	-	Melakukan sosialisasi mengenai pentingnya keamanan informasi.
INF-07	Adanya dokumen kontrak dengan *customer* dan materai terkait *awareness.*	-	Adanya sosialisasi terkait *awareness.*
INF-08	Terdapat NDA untuk pihak ketiga dan NDA individu, dan	-	Perlu disosialisasikan terkait *awareness* pihak ketiga.

Risk No	Rincian Rencana Pengendalian		
	Kebutuhan Dokumen	**Kebutuhan Teknologi**	**Kebutuhan Penunjang**
	materi *awarenesss* pihak ketiga.		
INF-09	Adanya dokumen yang berisikan informasi mengenai kepemilikan *asset.*	Adanya sistem *database* untuk data aset dan data file.	-
INF-10	Adanya dokumen kebijakan/prosedur mengenai klasifikasi informasi.	Adanya penyimpanan data sesuai tingkat rahasianya.	-
INF-11	Adanya kebijakan/prosedur mengenai klasifikasi informasi.	Sistem penyimpanan dokumen *soft copy* sesuai tingkat klasifikasi informasi tersebut.	Sistem penyimpanan dokumen *hard copy* sesuai tingkat klasifikasi informasi tersebut.
INF-12	Adanya SOP pemutusan hubungan kerja.	-	Dilakukan pemutusan akses untuk pegawai yang sudah tidak bisa bekerja, baik *Email* hingga akses ruangan.
INF-13	Adanya kebijakan atau prosedur mengenai pengamanan perlatan dan prosedur mengenai mekanisme pelaporan kehilangan perangkat	-	Adanya informasi mengenai prosedur pelaporan kehilangan perangkat khususnya pada pegawai baru.
INF-14	Adanya kebijakan atau prosedur mengenai media penyimpanan yang digunakan kembali.	Adanya media penyimpanan khusus penggunaan ulang media.	-
INF-15	Adanya prosedur operasi berupa intruksi kerja.	-	Adanya sosialisasi atau simulasi mengenai prosedur instruksi kerja dalam pemrosesan data/informasi.
INF-16	Adanya prosedur dalam mekanisme *backup*	Sudah dilakukan *backup* di luar data *center*, Melakukan *backup online*.	-
INF-17	Adanya prosedur atau mekanisme pelaporan jika terjadi serangan virus.	Adanya server antivirus.	Adanya sosialisasi mengenai *management knowledge*.
INF-18	Adanya prosedur kontrol keamanan penggunaan internet.	Adanya server antivirus.	Adanya sosialisasi mengenai cara mengatasi kontrol keamanan penggunaan internet.
INF-19	Adanya peraturan mengenai penggunaan *software.*	Adanya server antivirus.	Adanya pengamanan *software* agar tidak ada software bajakan yang masuk.

Risk No	Rincian Rencana Pengendalian		
	Kebutuhan Dokumen	**Kebutuhan Teknologi**	**Kebutuhan Penunjang**
INF-20	Adanya kebijakan dalam pembuatan *mobile code*	Adanya *security policy* untuk *mobile code.*	-
INF-21	Adanya peraturan dalam melakukan *backup* data atau informasi.	-	Dilakukan *backup* secara rutin
INF-22	Adanya peraturan dalam melakukan backup data atau informasi	-	Dilakukan *backup* secara rutin
INF-23	Adanya peraturan dalam melakukan *backup* data atau informasi.	-	Dilakukan *backup* secara rutin.
INF-24	Adanya kebijakan mengenai kontrol jaringan.	Menggunakan *firewall*, IPS/IDS untuk *control network* dan melakukan konfigurasi jaringan	-
INF-25	Adanya kebijakan mengenai pengelolaan *removable* media	Adanya autentikasi sebelum melakukan *removable* media	-
INF-26	Adanya kebijakan yang mengatur pembuangan media.	Adanya autentikasi sebelum melakukan pembuangan media.	-
INF-28	Adanya perjanjian pertukaran informasi untuk data rahasia.	Perlu dilakukan kontrol terkait penukaran informasi secara rutin.	-
INF-29	Adanya prosedur mekanisme dalam pengiriman dan penerimaan media fisik.	Adanya pengamanan yang dilakukan terhadap media fisik di data *center*.	Adanya *security* di daerah data *center.*
INF-30	Adanya kebijakan atau prosedur yang mengatur mengenai pengiriman informasi	-	-
INF-31	Adanya kebijakan dan prosedur mengenai interkoneksi sistem informasi bisnis	Adanya proteksi keamanan dalam mengirimkan informasi	-
INF-35	Adanya kebijakan/prosedur pengelolaan password	-	Adanya sosialiasi mengenai pengelolaan password yang digunakan
INF-36	Adanya kebijakan/prosedur pengelolaan password	-	Adanya sosialiasi mengenai pengelolaan password yang digunakan dan pentingnya menjaga keamanan informasi
INF-37	Adanya kebijakan clean desk dan clear screen	Menerapkan clean desk dan clear screen	
INF-39	Adanya kebijakan mengenai BCP/DRP		Sudah dilakukan pengujian

Risk No	Rincian Rencana Pengendalian		
	Kebutuhan Dokumen	**Kebutuhan Teknologi**	**Kebutuhan Penunjang**
INF-44	Dilakukannya pendataan aset database dan data file secara berkala	Database data dan file	-
INF-47	Terdapat backup pada CCTV	Adanya CCTV	-
INF-48	Terdapat backup pada CCTV	Adanya CCTV	-
INF-49	Terdapat backup pada CCTV	Adanya CCTV	-
INF-50	Adanya peraturan mekanisme dalam melakukan pengecekan atau kontrol CCTV	Adanya CCTV	Adanya pengecekan kontrol perangkat CCTV secara bekala
INF-51	Adanya logbook tamu	-	Adanya security
INF-52	-	Log CCTV sudah diamankan	
INF-53	-	Adanya jam data center, finger print dan CCTV	
INF-54	-	-	Melakukan kontrol diseluruh perangkat yang ada
INF-55	Adanya kebijakan terkait sistem keamanan informasi	-	-
INF-56	Adanya kebijakan terkait sistem keamanan informasi	-	-
INF-57	Adanya struktur organisasi SMKI	-	-
INF-58	Adanya struktur organisasi SMKI	-	-
INF-59	Adanya surat pernyataan kerahasiaan perusahaan	-	-
INF-60	-	Adanya aset database dan data file	-
INF-61	-	Adanya aset database dan data file	-
INF-62	Adanya kebijakan/prosedur mengenai klasifikasi informasi	-	-
INF-63	Adanya kebijakan/prosedur mengenai klasifikasi informasi	-	-
INF-64	Adanya prosedur mekanisme pihak ketiga untuk memasuki area kerja	Adanya kartu akses khusus atau facedoor untuk memasuki ruang kerja	Terdapat petugas keamanan dan resepsionis di lobby
INF-65	Adanya dokumen kontrol yang disimpan pada tempat yang aman	Adanya proteksi ruang penyimpanan	-
INF-66	Adanya aturan terkait pengamanan dokumen kontrak	-	-

Risk No	Rincian Rencana Pengendalian		
	Kebutuhan Dokumen	**Kebutuhan Teknologi**	**Kebutuhan Penunjang**
INF-67	Adanya kebijakan mengenai proteksi informasi/data/dokumen	Adanya akses card untuk memasuki ruangan	Adanya petugas keamanan Gudang
INF-68	Adanya kebijakan mengenai area umum, terbatas dan aman	-	-
INF-69	Adanya kebijakan clean desk dan clear screen	Menerapkan clear desk dan clear screen	-
INF-70	Adanya kebijakan terkait BCP/DRP	Melakukan pengujian terkait BCP/DRP	-
INF-71	Adanya dokumen mengenai aturan terkait pengamanan dokumen-dokumen	Perlu adanya proteksi dalam penyimpanan informasi	-
INF-72	Adanya kebijakan/prosedur mengenai klasifikasi informasi	Adanya keamanan terhadap dokumen-dokumen menggunakan password dll untuk mengakses dokumen tersebut	-
INF-73	Adanya kebijakan/prosedur mengenai klasifikasi informasi	Adanya keamanan terhadap dokumen-dokumen menggunakan password dll untuk mengakses dokumen tersebut	-
INF-74	Adanya kebijakan mengenai area umum, terbatas, dan aman	Adanya keamanan terhadap dokumen-dokumen menggunakan password dll untuk mengakses dokumen tersebut	-
INF-75	Adanya kebijakan clean desk dan clear screen	Menerapkan clear desk dan clear screen	-
INF-76	Adanya kebijakan clean desk dan clear screen	Menerapkan clear desk dan clear screen	-
INF-77	Adanya kebijakan mengenai pengelolaan removable media	Adanya kebijakan mengenai pengelolaan removable media	-
INF-78	Adanya kebijakan yang mengatur pembuangan media	Adanya kebijakan mengatur pembuangan media	-
INF-79	Adanya kebijakan terkait NDA pihak ketiga dan individu]	-	-
INF-80	Adanya peraturan mengenai kntor akses fisik ke ruang kerja	Adanya facedoor atau kartu akses untuk mengakses ruangan tersebut	-
INF-81	Adanya kebijakan mengenai pengelolaan removable media	-	Perlu dilakukan pengecekan terhadap setiap USB Flashdisk
INF-82	-	Adanya server antivirus	Adanya sosialiasi cara mengatasi atau menangani agar tidak terserang virus

Risk No	Rincian Rencana Pengendalian		
	Kebutuhan Dokumen	**Kebutuhan Teknologi**	**Kebutuhan Penunjang**
INF-83	Adanya prosedur pengimplementasian deep discovery email untuk mengatasi agar email tidak terserang virus	Adanya implementasi deep discovery	Adanya sosialiasi cara mengatasi atau menangani agar email tidak terserang virus

2) Risk Assessment Perangkat Keras

Berikut table 3.8 *risk assessment* terkait perangkat keras yang berisikan rincian rencana pengendalian, seperti kebutuhan dokumen, kebutuhan teknologi, dan kebutuhan penunjang.

Table 3.8 Risk Assessment Perangkat Keras

Risk No	Rincian Rencana Pengendalian		
	Kebutuhan Dokumen	**Kebutuhan Teknologi**	**Kebutuhan Penunjang**
PHY-01	Adanya prosedur dalam penggunaan alat pendeteksi kebakaran	Adanya fire extinguisher, smoke detector, fire supression pada ruang data center	Melakukan maintenance secara berkala
PHY-02	Adanya kebijakan BCP/DRP	-	Melakukan pengujian terhadap BCP/DRP
PHY-03	Adanya prosedur pengamanan fisik data center	Adanya proteksi keamanan pada data center	Adanya security yang berjaga
PHY-04	Adanya buku tamu, adanya standard atau kebijakan akses ke data center	Adanya CCTV, Access door di data center	Adanya security atau resepsionis yang berjaga
PHY-05	Adanya kebijakan mengenai pembagian area umum, terbatas dan aman	Adanya accessdoor dan CCTV di setiap area	-
PHY-06	Adanya kebijakan mengenai keamanan informasi.	-	Melakukan sosialisasi terkait *awareness* keamanan informasi.
PHY-07	Adanya kebijakan yang berisikan struktur dan tanggung jawab keamanan informasi.	Adanya CCTV di setiap ruangan.	-
PHY-08	Adanya kebijakan terkait akses ke arah terbatas dan aman.	Adanya CCTV, *access door* di setiap area.	-

Risk No	Rincian Rencana Pengendalian		
	Kebutuhan Dokumen	**Kebutuhan Teknologi**	**Kebutuhan Penunjang**
PHY-09	Adanya prosedur mengenai mekanisme untuk dapat mengakses area tersebut.	Adanya *access door* ke ruang data *center*, adanya CCTV.	-
PHY-10	Adanya kebijakan terkait akses ke arah terbatas dan aman.	Adanya CCTV, *access door* di setiap area.	-
PHY-11	-	Media penyimpanan server yang aman dan rapi.	Adanya rak yang memiliki kunci sendiri.
PHY-12	-	Adanya UPS dan Genset.	Adanya pengecekan berkala pada UPS dan Genset.
PHY-13	Sudah dilakukan *maintenance.*	-	-
PHY-14	Adanya kebijakan dan prosedur mengenai *change management.*	-	Dilakukan pengecekan perangkat secara berkala.
PHY-15	Adanya standar prosedur penggunaan perangkat.	Setiap perangkat terdapat manual penggunaan.	-
PHY-16	Adanya kebijakan dan prosedur mengenai *change management.*	Dibuat standar kapasitas *system*.	-
PHY-17	Adanya kebijakan terkait pengamanan perangkat penyimpan informasi.	Adanya perangkat yang mendeteksi lingkungan *data center.*	-
PHY-18	-	Audit logging sudah diaktifkan	-
PHY-19	-	Adanya *tools* monitoring	Adanya sosialisasi terkait penanganan atau pencegahan pengolahan informasi
PHY-20	-	Dilakukannya *backup* log	Adanya sosialisasi terkait perlindungan atau pencurian data
PHY-21	Adanya pencatatan aktivitas *administrator*	Adanya *operator* dan *administrator* di masing-masing *server*	-
PHY-22	-	Melakkan pengumpulan terhadap *fault* log	-
PHY-23	-	Adanya CCTV pada *server* dan laptop, *fingerprint* dan *access door.*	-
PHY-24	Adanya buku tamu, dan kebijakan mengenai pencurian perangkat.	Adanya CCTV, *access door.*	-

Risk No	Rincian Rencana Pengendalian		
	Kebutuhan Dokumen	**Kebutuhan Teknologi**	**Kebutuhan Penunjang**
PHY-25	Adanya prosedur dalam penggunaan alat pendeteksi kebakaran.	Adanya *fire extinguisher*, *sprinkler*, *smoke detector.*	Melakukan *maintenance* secara berkala.
PHY-26	Adanya list nama perangkat *network.*	Kepemilikan perangkat *network* yang telah ditetapkan.	-
PHY-27	Adanya peraturan untuk memasuki data *center*.	Adanya *access door* dan CCTV di ruangan.	Adanya *security* yang menjaga.
PHY-28	-	Adanya akses masuk melalui mekanisme biometric.	-
PHY-29	-	Adanya *fire extinguisher, sprinkler,* dan *smoke detector.*	-
PHY-30	Adanya peraturan mengenai data *center* seperti ketentuan bertamu.	Adanya *access door* dan CCTV.	-
PHY-31	Adanya peraturan mengenai data *center* seperti ketentuan bertamu.	Adanya *access door* dan CCTV.	-
PHY-32	Ada prosedur untuk keluar masuk data *center.*	Adanya CCTV.	-
PHY-33	Adanya ruangan khusus untuk media penyimpanan perangkat.	Adanya proteksi keamanan.	-
PHY-34	Adanya kebijakan mengenai perencanaan infrastruktur.	Dilakukan pemisahan antara kabel dan kabel daya.	-
PHY-35		Dilakukan monitoring.	-
PHY-36	Adanya dokumentasi *operating procedure.*	-	-
PHY-37	Adanya prosedur *change management.*	Melakukan dokumentansi perubahan konfigurasi.	-
PHY-38	Perlu dilakukan *review* dan *planning*.	Adanya monitoring kapasitas menggunakan *sistem*.	-
PHY-39	Melakukan *review* secara rutin terhadap *security* log.	Adanya IPS, *firewall* dan IDS. Dilakukan juga VA secara berkala.	-
PHY-40	Melakukan *review* secara rutin terhadap *security* log.	Adanya IPS, *firewall* dan IDS. Dilakukan juga VA secara berkala.	-

Risk No	Rincian Rencana Pengendalian		
	Kebutuhan Dokumen	**Kebutuhan Teknologi**	**Kebutuhan Penunjang**
PHY-41	Melakukan review secara rutin terhadap *security* log.	Adanya IPS, *firewall* dan IDS. Dilakukan juga VA secara berkala.	-
PHY-42	-	Melakukan pengelolaan dan konfigurasi *network.*	-
PHY-43	-	Melakukan pengelolaan dan konfigurasi *network.*	-
PHY-44	Adanya *policy network.*	Melakukan pengendalian user terhadap akses *network.*	-
PHY-45	-	Terdapat *active directory.*	-
PHY-46	Adanya kebijakan akses *control.*	Terdapat *active directory.*	-
PHY-47	Adanya dokumen yang berisikan pembagian *network* yang jelas	Dilakukan segmentasi pada *network* dan melakukan identifikasi perangkat pada *network.*	-
PHY-48	Adanya dokumen yang berisikan pembagian *network* yang jelas.	Dilakukan pemisahan antara kabel data dan kabel daya.	-
PHY-49	Adanya dokumen yang berisikan pembagian *network* yang jelas dalam setiap area.	Dilakukan segmentasi pada *network* dan melakukan identifikasi perangkat pada *network.*	-
PHY-50	-	Dilakukan segmentasi pada *network* dan dilakukan pengendalian *routing* pada *network.*	-
PHY-51	-	Adanya *active directory* dan VPN.	-
PHY-52	-	Dilakukan segmentasi pada *network.*	-
PHY-53	-	Adanya *access door* dan CCTV.	-
PHY-54	Adanya prosedur dalam penggunaan alat pendeteksi kebakaran.	Adanya *fire extinguisher*, *smoke detector* dan *fire supression* pada ruang data *center.*	Melakukan *maintenance* secara berkala.
PHY-55	Adanya pedoman mengenai penggunaan *asset.*	-	-
PHY-56	Adanya list kepemilikan *storage* yang telah ditetapkan.	Media penyimpanan *asset*.	-

Risk No	Rincian Rencana Pengendalian		
	Kebutuhan Dokumen	**Kebutuhan Teknologi**	**Kebutuhan Penunjang**
PHY-57	Adanya kebijakan terkait akses data *center.*	Adanya akses masuk melalui mekanisme *biometric.*	-
PHY-58	Adanya prosedur dalam penggunaan alat kebakaran.	Adanya *fire extinguisher, sprinkler, smoke detector.* Perlu menerapkan *fire suppresser*.	-
PHY-59	Adanya peraturan mengenai data *center* seperti ketentuan bertamu.	Adanya *access door* dan CCTV.	-
PHY-60	Adanya peraturan mengenai data *center* seperti ketentuan bertamu.	Adanya *access door* dan CCTV.	-
PHY-61	Adanya prosedur mengenai mekanisme untuk dapat keluar masuk area tersebut.	Adanya *access door* ke ruang data *center*, adanya CCTV.	-
PHY-62	Kebijakan dalam penyimpanan perangkat.	Adanya rak yang terkunci dan terkontrol.	-
PHY-63	Kebijakan dalam melakukan pemeliharaan perangkat.	Dilakukan *monitoring storage.*	-
PHY-64	Adanya prosedur *change management*.	Melakukan dokumentasi perubahan konfigurasi.	-
PHY-65	Adanya standar prosedur *storage.*	Adanya *storage* perangkat.	-
PHY-66	Adanya prosedur *capacity planning*	Perlu dilakukan *capacity planning* untuk *storage*	-
PHY-67	Adanya kebijakan terkait pengamanan perangkat penyimpan informasi.	Adanya pengamanan media fisik di lingkungan data *center*.	-
PHY-68	Adanya list kepemilikan *asset*.	Kepemilikan aset yang telah ditetapkan.	-
PHY-69	Kebijakan dalam pemeliharaan perangkat pendukung.	Melakukan *maintenance* perangkat pendukung yang dilakukan berkala.	-
PHY-70	Adanya prosedur penggunaan alat pendeteksi dan pemadaman api.	*Adanya fire extinguisher, sprinkler, smoke detector* pada Gedung.	-
PHY-71	Adanya kebijakan *backup* data *personal.*	Adanya proteksi perangkat.	-
PHY-72	Adanya kebijakan pengamanan area kerja.	Adanya CCTV di seluruh area lingkungan kerja.	Adanya petugas keamanan.

Risk No	Rincian Rencana Pengendalian		
	Kebutuhan Dokumen	**Kebutuhan Teknologi**	**Kebutuhan Penunjang**
PHY-73	Adanya kebijakan akses ke area umum, terbatas, dan aman.	Adanya *access door* di setiap area.	-
PHY-74	Adanya kebijakan area umum, terbatas dan aman	Adanya *access door* dan CCTV di setiap area	-
PHY-75	Adanya kebijakan terkait pencurian atau kehilangan perangkat atau data.	-	Melakukan sosialisasi *awareness* mengenai keamanan informasi.
PHY-76	Adanya kebijakan terkait struktur dan tanggung jawab mengenai keamanan informasi.	Adanya CCTV dan *access door*	Adanya *security*
PHY-77	-	Adanya accessdoor ketika masuk area terbatas	Adanya resepsionis
PHY-78	Adanya kebijakan pengamanan pada perangkat yang dibawa keluar area.	Adanya CCTV untuk menangani kehilangan perangkat.	-
PHY-79	Adanya kebijakan *clean desk policy.*	Menerapkan *clean desk* dan *clean screen.*	-
PHY-80	SOP pemutusan hubungan kerja, adanya *form employee exit checklist.*	Pemutusan akses *door.*	-
PHY-81	SOP pemutusan hubungan kerja, adanya *form employee exit checklist.*	Pemutusan akses *door.*	-
PHY-82	-	Pengamanan akses *remote* melalui VPN dan pembatasan pengguna VPN berdasarkan kebutuhan.	-
PHY-83	Adanya prosedur terkait cara penanganan perangkat rusak.	*Hotline service desk.*	-
PHY-84	-	Log tersebar di beberapa perangkat.	Melakukan implementasi SIEM.
PHY-85	Adanya kebijakan mengenai *firewall.*	Melakukan *review firewall* secara berkala, menggunakan VPN.	-
PHY-86	-	Log tersebar di beberapa perangkat.	Melakukan implementasi SIEM.

3) Risk Assessment Perangkat Lunak

Berikut table 3.8 *risk assessment* terkait perangkat lunak yang berisikan rincian rencana pengendalian, seperti kebutuhan dokumen, kebutuhan teknologi, dan kebutuhan penunjang.

Table 3.9 Risk Assessment Perangkat Lunak

Risk No	**Rincian Rencana Pengendalian**		
	Kebutuhan Dokumen	**Kebutuhan Teknologi**	**Kebutuhan Penunjang**
SOF-01	Adanya dokumen kebijakan keamanan informasi.	-	Adanya sosialisasi terkait *awareness* dalam keamanan informasi data melalui aplikasi.
SOF-02	Adanya dokumen kebijakan keamanan informasi.	-	Adanya sosialisasi terkait *awareness* dalam keamanan informasi data melalui aplikasi.
SOF-03	Adanya kebijakan terkait kelemahan *system.*	-	Adanya personil yang mengikuti *special interest group.*
SOF-04	Adanya kebijakan terkait kepemilikan aset dan list kepemilikan aset.	Adanya *database* aset dan data.	-
SOF-05	Adanya SOP pemutusan hubungan kerja.	Pemutusan *access card* dll.	-
SOF-06	Adanya kebijakan *change management.*	Melakukan dokumentasi terkait perubahan konfigurasi.	-
SOF-07	Adanya kebijakan *change management.*	Melakukan dokumentasi terkait perubahan konfigurasi.	-
SOF-08	Adanya kebijakan pemakaian *source code.*	Menggunakan *software versioning.*	-
SOF-09	-	Terdapat 2 *server* untuk *development* dan *production.*	Terdapat *stage development.*
SOF-10	-	Adanya antivirus *server.*	Perlu dilakukan pengecekan berkala pada aplikasi.
SOF-11	-	Adanya antivirus *server.*	Perlu dilakukan kontrol keamanan terhadap penggunaan internet.
SOF-12	Adanya kebijakan.	Adanya *access matrix.*	-
SOF-13	Adanya kebijakan mengenai *password* dan standar *policy user access.*	Adanya *user* akses seperti ID atau autentikasi.	Melakukan sosialisasi terkait penggunaan *password.*

Risk No	Rincian Rencana Pengendalian		
	Kebutuhan Dokumen	**Kebutuhan Teknologi**	**Kebutuhan Penunjang**
SOF-14	Adanya kebijakan mengenai *password* dan standar *policy user access.*	Adanya *user* akses seperti ID atau autentikasi.	Melakukan sosialisasi terkait penggunaan *password.*
SOF-15	Adanya kebijakan mengenai *password* dan standar *policy user access.*	Implementasi *policy* mengenai *password expired.*	-
SOF-16	Adanya kebijakan mengenai *password* dan standar *policy user access.*	Implementasi *policy* mengenai *password expired*.	-
SOF-17	Adanya kebijakan mengenai password dan standar policy user access.	Implementasi *policy* mengenai password expired.	-
SOF-18	-	Sudah terdapat pada aplikasi	-
SOF-19	-	Ada *patch management* untuk OS dan aplikasi.	-
SOF-20	Adanya SOP insiden terkait *security*.	-	Adanya sosialisasi mengenai penanganan insiden keamanan, misal jika terjadi *hacking*.
SOF-21	-	VA sudah dilakukan secara berkala, implementasi aqunetix, pentest secara berkala.	-
SOF-22	-	-	Adanya personil yang mengikuti *special* interest *group*.
SOF-23	Materi *awareness antivirus server.*	Adanya *antivirus server.*	Adanya sosialisasi terkait awareness antivirus server.
SOF-24	Adanya kebijakan *password* dan standar policy *user access.*	Adanya *user* access.	Adanya standar policy user access.
SOF-25	Adanya kebijakan *password* dan standar *policy user access.*	Adanya *user access.*	Adanya standar *policy user access.*
SOF-26	Adanya kebijakan *password.*	Adanya *user access.*	Adanya standar *policy user access.*
SOF-27	Adanya kebijakan mengenai *password* yang sudah ada.	-	Adanya sosialisasi terkait awareness mengenai keamanan menjaga *password.*
SOF-28	-	Pengecekan kontrol sistem dilakukan secara rutin.	Sudah terdapat personil yang mengikuti *special interest group.*
SOF-29	-	Pengecekan kontrol sistem dilakukan secara rutin.	Sudah terdapat personil yang mengikuti *special interest group.*

Risk No	Rincian Rencana Pengendalian		
	Kebutuhan Dokumen	**Kebutuhan Teknologi**	**Kebutuhan Penunjang**
SOF-30	Adanya prosedur penting dalam menjalankan sistem yang sudah tersedia dan ditetapkan.	-	-
SOF-31	Adanya kebijakan dan prosedur change management.	-	Perlu adanya dokumentasi apabila adanya perubahan.
SOF-32	Adanya kebijakan dan prosedur *change management.*	-	Perlu adanya dokumentasi apabila adanya perubahan.
SOF-33	Adanya prosedur *access control* dan struktur organisasi, serta peran & tanggung jawab terkait SMKI.	-	-
SOF-34	-	Adanya virus *server.*	-
SOF-35	-	Adanya virus *server.*	-
SOF-36	-	Adanya akses ke dalam *server.*	-
SOF-37	-	Adanya akses kedalam *server* melalui OAM.	-
SOF-38	Kebijakan mengenai *user account.*	-	-
SOF-39	Kebijakan mengenai pengelolaan *password.*	-	Perlu adanya sosialisasi terkait *awareness* dalam pengelolaan *password.*
SOF-40	Adanya mekanisme dilakukannya *session time out.*	Adanya *session time out* pada aplikasi.	-
SOF-41	-	Adanya *patch management*	-
SOF-42	-	Adanya *patch management* dan *virtual patch* dari *depsecurity.*	-
SOF-43	-	Adanya *access matrix.*	-
SOF-44	-	Adanya *server* antivirus.	-
SOF-45	Adanya prosedur mengenai pemberian fasilitas terdapat *whitelist.*	-	-
SOF-46	Materi terkait *awareness* dari *user* mengenai *email phishing.*	Implementasi Qradar untuk monitoring *incident.*	Melakukan sosialisasi *awareness* rutin ke *user*, terdapat *team monitoring* dan menangani *incident security.*
SOF-47	Adanya peraturan mengenai akses log dan mekanisme dalam melakukan *review* log akses.	Review log akses dan hak akses secara berkala.	-

Risk No	Rincian Rencana Pengendalian		
	Kebutuhan Dokumen	**Kebutuhan Teknologi**	**Kebutuhan Penunjang**
SOF-48	Adanya prosedur *instalasi software non-standard.*	Melakukan reset *password* secara berkala dan monitoring instalansi *software* dengan SCCM.	-
SOF-49	Kebijakan terkait mengakses *resource internal* perusahaan saat WFH.	Memanfaatkan *device* F5 *existing*.	-
SOF-50	Adanya kebijakan terkait pelanggaran penggunaan *software* illegal.	Melakukan audit *software* secara rutin.	Adanya *awareness* ke *user* untuk mereset *password* admin.

4) Risk Assessment Sarana

Berikut table 3.10 *risk assessment* terkait sarana yang berisikan rincian rencana pengendalian, seperti kebutuhan dokumen, kebutuhan teknologi, dan kebutuhan penunjang.

Table 3.10 Risk Assessment Sarana

Risk No	Rincian Rencana Pengendalian		
	Kebutuhan Dokumen	**Kebutuhan Teknologi**	**Kebutuhan Penunjang**
SUP-01	Dokumen mengenai list kepemilikan aset dan nama aset dan dokumen perjanjian mengenai penggunaan asset.	-	Adanya prosedur untuk menangani fasilitas atau aset yang mengalami kerusakan.
SUP-02	Adanya dokumen mengenai prosedur pemeliharaan fasilitas dengan baik dan peraturan pemeliharaan fasilitas.	-	Adanya sosialiasi mengenai cara pemeliharaan fasilitas.
SUP-03	Adanya dokumen mengenai prosedur pemeliharaan fasilitas dengan baik dan peraturan pemeliharaan fasilitas.	-	Adanya sosialiasi mengenai cara pemeliharaan fasilitas.
SUP-04	Adanya dokumen mengenai kebijakan dalam pengamanan saat terjadi pemogokan.	-	Adanya prosedur mekanisme pelaporan fasilitas yang tidak dapat digunakan.
SUP-05	Adanya dokumen kepemilikan *asset.*	-	Adanya dokumen mengenai mekanisme penanganan perangkat yang rusak dan

Risk No	Rincian Rencana Pengendalian		
	Kebutuhan Dokumen	**Kebutuhan Teknologi**	**Kebutuhan Penunjang**
			mekanisme pelaporan kehilangan perangkat.
SUP-06	Adanya peraturan mengenai pelaksanaan *maintenance* perangkat.	*Maintenance* perangkat pendukung sudah dilakukan berkala.	-
SUP-07	Adanya dokumen kepemilikan *asset.*	-	Adanya dokumen mengenai mekanisme penanganan perangkat yang rusak dan mekanisme pelaporan kehilangan perangkat.
SUP-08	Adanya peraturan mengenai kerusakan perangkat dan prosedur mekanisme untuk menangani perangkat yang rusak.	Kotak pengaman.	-
SUP-09	Adanya aturan pengecekan kontrol perangkat secara berkala.	Melakukan *maintenance* perangkat pendukung yang dilakukan berkala.	-
SUP-10	Adanya dokumen kepemilikan asset.	-	Adanya dokumen mengenai mekanisme penanganan perangkat yang rusak dan mekanisme pelaporan kehilangan perangkat.
SUP-11	Adanya prosedur mengenai pemeliharaan fasilitas.	Adanya *maintenance* fasilitas pendukung yang dilakukan secara berkala.	-
SUP-12	Adanya prosedur mengenai pemeliharaan fasilitas.	Adanya *maintenance* fasilitas pendukung yang dilakukan secara berkala.	-
SUP-13	Adanya kebijakan BCP/DRP dan melakukan *testing.*	-	Adanya *security* dan pihak kepolisian jika terjadi pemogokan atau huru hara.

5) Risk Assessment Pihak Ke-3

Berikut table 3.7 *risk assessment* terkait informasi yang berisikan rincian rencana pengendalian, seperti kebutuhan dokumen, kebutuhan teknologi, dan kebutuhan penunjang.

Table 3.11 Risk Assessment Pihak Ke-3

Risk No	Rincian Rencana Pengendalian		
	Kebutuhan Dokumen	**Kebutuhan Teknologi**	**Kebutuhan Penunjang**
SER-01	Adanya dokumen perjanjian SLA.	-	Perlu mencari vendor yang sesuai dengan kebutuhan.
SER-02	Adanya dokumen perjanjian terkait keamanan informasi yang ada.	-	Adanya sosialisasi mengenai pengamanan informasi (cara mencegah dan cara menjaga keamanan informasi).
SER-03	-	-	Perlu mencari vendor yang sesuai dengan kebutuhan.
SER-04	Adanya dokumen SLA dan dokumen standar layanan yang disepakati oleh perusahaan.	-	Perlu mencari vendor yang sesuai dengan kebutuhan.
SER-05	Sudah terdapat SLA.	-	Perlu mencari vendor yang sesuai dengan kebutuhan.
SER-06	Adanya perjanjian keamanan informasi yang ada.	-	-
SER-07	Melakukan review SLA.	-	-
SER-08	Adanya perjanjian keamanan informasi yang ada.	-	-
SER-09	Adanya kebijakan terkait screening dan adanya prosedur mekanisme dalam seleksi tenaga *outsource.*	-	-
SER-10	Adanya perjanjian kerahasiaan level perusahaan dan individu yang menjadi persyaratan jasa tenaga *outsource*.	Perlu adanya pengamanan agar personil tidak bisa melakukan pembocoran informasi rahasia.	Adanya sosialisasi mengenai koordinasi dan peran tangggung jawab setiap personal.
SER-11	-	Adanya relokasi kabel FO di area HO.	-

6) Risk Assessment Intangible

Berikut table 3.12 *risk assessment* terkait *intangible* yang berisikan rincian rencana pengendalian, seperti kebutuhan dokumen, kebutuhan teknologi, dan kebutuhan penunjang.

Table 3.12 Risk Assessment Intangible

Risk No	**Rincian Rencana Pengendalian**
	Kebutuhan Dokumen
INT-01	Adanya kebijakan sistem manajemen keamanan informasi.
INT-02	Adanya kebijakan sistem manajemen keamanan informasi.
INT-03	Adanya SLA dengan vendor.
INT-04	Adanya kebijakan BCP/DRP.
INT-05	Adanya dokumen terkait peraturan perundangan yang berlaku apabila terjadi pelanggaran keamanan informasi.
INT-06	Adanya pedoman mutu.

3.1 Kendala yang Ditemukan

Dalam melakukan suatu pekerjaan atau tugas, pastilah tidak semua hal dapat berjalan dengan lancar dan sesuai dengan ekspetasi penulis. Terkadang dalam mengerjakan tugas atau melakukan pekerjaan, ada kendala atau hal yang dapat menghambat proses dalam menyelesaikan pekerjaan atau tugas. Ada beberapa kendala yang dihadapi oleh penulis selama melaksanakan praktek kerja magang sebagai divisi *IT Governance* dan *Security* diantaranya:

1. Kendala pertama yang dihadapi yaitu tidak adanya komunikasi dari pembimbing mengenai penjelasan dalam pengerjaan tugas yang diberikan kepada penulis.
2. Kendala kedua yang dihadapi yaitu tidak adanya *tool project management* yang berisikan detail tugas dan deadline dari tugas yang diberikan.
3. Kendala ketiga yang dihadapi yaitu tidak adanya bimbingan atau diskusi mengenai tugas atau pekerjaan yang sedang dikerjakan.
4. Kendala keempat yaitu belum mempelajari *framework* ISO 27001 saat perkuliahan, sehingga saat kesulitan dalam melaksanakan praktek kerja magang.

3.2 Solusi atas Kendala yang Ditemukan

Kendala yang ada selama pelaksanaan kerja magang di PT. United Tractors Tbk membuat penulis menjadi kurang efektif dan merasa kesulitan, maka dari itu penulis menanganinya agar program kerja magang menjadi lebih baik lagi. Adapun solusi untuk kendala yang ada diantaranya:

1. Solusi untuk kendala pertama yaitu aktif dalam mencari informasi sendiri dalam mengerjakan suatu pekerjaan atau tugas yang diberikan oleh pembimbing.
2. Solusi untuk kendala kedua yaitu membuat *tool project management* sendiri mengenai list tugas yang diberikan.
3. Solusi untuk kendala ketiga yaitu melakukan pertemuan atau diskusi melalui daring maupun secara langsung.
4. Solusi untuk kendala keempat yaitu saat perkuliahan juga mempelajari *framework* ISO karena beberapa perusahaan sudah menerapkan *framework* tersebut.