Re-Assessment Konsistensi Dokumen Kontrol Sertifikasi ISO 27001:2013 (ISMS) di Bagian Komunikasi Satelit Monitoring PT. Bank BRI, TBK

Sigit Tri Yuwono[1], Nanang Pratama[2], Vivi Afifah[3]

[1,3]Institut Teknologi dan Bisnis Bank Rakyat Indonesia
[2]Divisi IT Infrastructure & Operations PT. Bank BRI, TBK
Pasar Minggu, Jakarta Selatan
E-mail : sigitt@gmail.com[1], nanang.pratama70@yahoo.co.id[2], vivi.afifah@bri-institute.ac.id[3]

ABSTRAK

Pada masa digitalisasi dan *big data analysis*, untuk organisasi atau perusahaan serangkaian aset informasi akan memiliki nilai yang sangat kritis sehingga harus dilindungi dari ancaman dan kerentanan keamanannya. *Information Security Management System* (ISMS) atau Sistem Manajemen Keamanan Informasi (SMKI) adalah seperangkat kebijakan dan prosedur untuk mengelola data sensitif organisasi secara sistematis, untuk melindungi serta menjaga kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*) aset-aset informasi tersebut. Divisi IT Infrastructure & Operations PT. Bank BRI, Tbk khususnya Departement Satellite Service Operations (SSO) secara organisasi telah menerapkan SMKI pada tata kelola IT dan operasional nya dan juga telah diakui baik internasional maupun secara nasional dengan memperoleh sertifikasi ISO 27001:2013 (ISMS) sejak tahun 2020. Sertifikasi tersebut pada pelaksanaan nya memiliki kontrol konsistensi pelaksanaan dan perlunya *re-assessment* sehingga selalu sesuai dengan kebijakan yang telah ditetapkan dan pasal ketentuan sertifikasi.

Kata kunci : aset informasi, kebijakan dan prosedur, sistem manajemen keamanan informasi (SMKI), ISO/IEC 27001:2013, sertifikasi, *re-assessment.*

ABSTRACT

Within digitalization and big data analysis environment, series of information assets will have a very critical value for an organization or company, so they must be protected from threats and security vulnerabilities. Information Security Management System (ISMS) is a set of policies and procedures to systematically manage sensitive organizational data, to protect and maintain the confidentiality, integrity and availability of their information assets.IT Infrastructure & Operations Division of PT. Bank BRI, Tbk especially the Satellite Service Operations (SSO) Department as an organization has implemented the ISMS in IT governance and operations and has also been recognized both internationally and nationally by obtaining ISO 27001:2013 (ISMS) certification since 2020. The certification mentioned in its implementation, has control over the consistency and the needs of re-assessment therefore it is always in accordance with the policies that have been set and the article on certification provisions.

Keyword : *information asset, policy and procedure, information security management system (ISMS), ISO/IEC 27001:2013, certification, re-assessment*

1. PENDAHULUAN

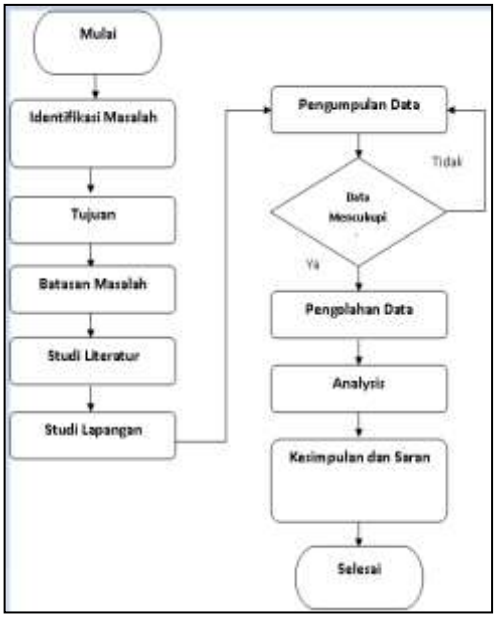
Divisi IT Infratructure & Operations Division khususnya pada Satellite Service Operations Departement sebagai organisasi yang telah mengadopsi standarisasi ISO 270001:2013 dalam kebijakan nya tentu tidak lepas dari kewajiban agar seluruh stakeholder dan seluruh team organisasi mulai dari karyawan dan jajaran management mengetahui, memahami, menerapkan, mematuhi, dan selalu melaksanakan prosedur manajemen kemananan informasi tersebut tidak terkecuali bagi anggota team pengganti, misalnya karyawan baru.

Hal lain yang menjadi perhatian adalah dalam berhubungan dengan rekanan, vendor, supplier, mitra kerja dan pihak ketiga lainya atau bahkan dengan pelanggan, terjadi pertukaran data atau informasi. Pertukaran ini atau yang sering disebut sebagai information exchange memerlukan kompromi agar masing-masing perusahaan saling menghormati dan sepakat bagaimana memperlakukan informasi tersebut agar tetap bernilai. Apabila perusahaan telah memiliki Sertifikasi ISO 27001, stakeholders akan lebih merasa nyaman untuk melakukan bisnis dan bahkan menjadi nilai tambah atau winning-factor ketika mengikuti tender bisnis tersebut. Akan tetapi jika rekanan, vendor, supplier, mitra kerja dan pihak ketiga tidak atau belum menerapkan standard yang sama maka harus adanya pernyataan kesepakatan serta *risk assessment* dan *non disclosure agreement* sesuai kebutuhan agar tetap memenuhi syarat dengan kebijakan manajemen keamanan informasi yang telah ditetapkan.

Selain itu sejak gelombang pandemi Covid-19 melanda dunia pada bulan Maret tahun 2020, *Work From Home* (WFH) menjadi solusi bagi berbagai institusi atau perusahaan agar aktivi-tas sehari-hari tetap berjalan walaupun harus dikerjakan dari rumah. Oleh karena itu segala potensi celah keamanan dari adanya aktivitas WFH yang akan berdampak pada keamanan sistem komputer secara umum ataupun pencurian data dan informasi secara khusus harus mulai diperhatikan dengan serius dan diberikan solusinya. Dalam hal ini, peningkatan eduka-si dan kesadaran staf terhadap isu *cyber security* serta mitigasinya menjadi salah satu solusi yang harus diprioritaskan.

2. METODOLOGI

Penelitian ini hakekatnya melaporkan hasil pengamatan dan peninjauan. Adapun metodologi yang dilakukan dijelaskan pada diagram alur (*Flowchart*) berikut ini.

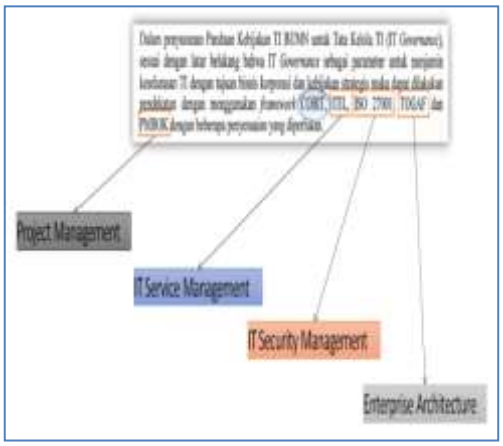


Gambar 1.
Flowchart Metodologi Laporan

3. LANDASAN TEORI

Panduan Tata Kelola, Sesuai PERMEN BUMN Tahun 2013

Tata kelola teknologi informasi (Bahasa Inggris: *IT governance*) adalah suatu cabang dari tata kelola perusahaan yang terfokus pada sistem teknologi informasi (TI) serta manajemen kinerja dan risikonya. Meningkatnya minat pada tata kelola TI sebagian besar muncul karena adanya prakarsa kepatuhan (seperti Sarbanes-Oxley di Amerika Serikat dan Basel II di Eropa) serta semakin diakuinya kemudahan proyek TI terhadap kinerja suatu organisasi. Tata kelola teknologi informasi menyediakan struktur untuk menyelaraskan strategi terknologi informasi dengan strategi bisnis.

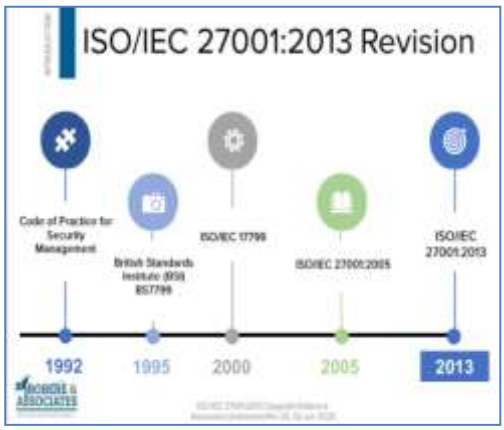


Gambar 2. Relevansi Framework Sertifikasi

Kebanyakan kerangka kerja tata kelola TI dirancang untuk membantu sebuah organisasi menentukan bagaimana divisi TI berfungsi secara keseluruhan, apa yang dibutuhkan oleh manajemen. Saat meninjau kerangka kerja, pertimbangkan budaya perusahaan. Apakah kerangka kerja atau model tertentu cocok untuk organisasi? Apakah sesuai dengan arahan para pemangku kepentingan? Bisa jadi kerangka kerja tersebut menjadi pilihan terbaik. Tetapi tentu saja sebuah organisasi dapat memilih menerapkan lebih dari satu kerangka kerja. Sebagai contoh, penerapan COBIT dan ITIL. Beberapa organisasi telah menggunakan COBIT dan COSO, bersama dengan standar ISO 27001 (untuk mengelola keamanan informasi).

SMKI berdasarkan ISO/IEC 27001

ISO/IEC 27001 adalah standar Keamanan Informasi (*information security*) yang diterbitkan oleh ISO (*International Organization for Standardization*) dan IEC (*International Electrotechnical Commission*) pada bulan Oktober 2005 yang menggantikan standar ISO/IEC 17799:2002 yang merupakan adopsi dari BS-7799 keluaran *British Standards Institute* pada tahun 90 an.

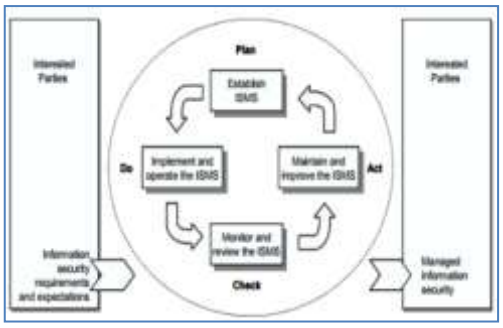


Gambar 3. Versi ISO/IEC 27001

Implementasi SMKI tidak hanya sekedar implementasi tanpa tindak lanjut. Sistem ini harus didukung dengan beberapa hal berikut untuk dapat diimplementasikan. Yaitu dengan dukungan perencanaan (*planning*), kebijakan keamanan (*security policy*), program (*prosedur*

dan proses), penilaian risiko (*risk assessment*) dan sumber daya manusia (*people*). ISO 27001 berisi mengenai persyaratan standar yang harus dipenuhi untuk membangun SMKI, ia juga mendefinisikan keperluan-keperluan untuk Sistem Manajemen Keamanan Informasi (SMKI) dan memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah organisasi dalam implementasi konsep keamanan informasi di organisasi.

Pendekatan proses yang didefinisikan ISO/IEC 27001 adalah siklus PDCA (*Plan-Do-Check-Act*) yang dapat diilustrasikan pada gambar berikut ini.



Gambar 4. Model PDCA
dalam Aplikasi Proses SMKI

1. **Plan** : Tahapan yang merupakan perencanaan dan perancangan SMKI. Seperti membangun komitmen, kebijakan, Kontrol, prosedur, instruksi kerja dan lainlain sehingga tercipta SMKI sesuai dengan keinginan.
2. **Do** : Tahapan pengimplemetasian dan operasi dari kebijakan, Kontrol, proses dan prosedur SMKI yang telah dibangun/ direncanakan pada tahapan plan.
3. **Chec**k : Tahapan yang membahas kegiatan monitoring pelaksanaan SMKI, termasuk melakukan evaluasi dan audit terhadap SMKI.
4. **Act** : Adalah tahapan kegiatan pengembangan (improvement) dimana di dalamnya merupakan kegiatan perbaikan dan pengembangan SMKI

Adapun Klausa dalam ISO/IEC 27001: 2013 terdiri dari 10 yaitu:

- **Klausa 1** – Ruang Lingkup Standar
- **Klausa 2** – Referensi Normatif
- **Klausa 3** – Ketentuan dan Definisi
- **Klausa 4** – Konteks Organisasi
- **Klausa 5** – Kepemimpinan
- **Klausa 6** – Perencanaan
- **Klausa 7** – Pendukung
- **Klausa 8** – Operasi
- **Klausa 9** – Evaluasi Kinerja
- **Klausa 10** – Peningkatan

Gambar 5. ANNEX (Klausa)/
Kerangka Standar Sistem Manajemen

4. HASIL DAN PEMBAHASAN

Sertifikasi ISO/IEC 27001:2013 oleh Robere & Asociate yang dilakukan pada tahun 2020 dilaksanakan sesuai kerangka penyusunan SMKI dengan siklus PDCA (*Plan-Do-Check-Act*), merencanakan, memeriksa prosedur, gap analysis, komitmen dari managemen, mengidentifikasi asset, resiko dan resiko (*PLAN*). Melakukan dan implementasi rencana yang telah dibuat sesuai dokumen kontrol kepatuhan terhadap prosedur (*DO*). Monitoring audit dan evaluasi terhadap yang telah dilaksanakan (*CHECK*). Serta saran dan rekomendasi untuk improvement (*ACT*). Sampai semua tahapan selesai dan memenuhi syarat maka Bagian Komunikasi Satelit Monitoring pada khususnya dan Departement Satellite Service Operations (SSO) pada umumnya, telah memenuhi syarat untuk mendapatkan sertifikasi tersebut.

Konsentrasi Rumusan Masalah:

A. Potensi anggota team baru yang belum memahami dan mematuhi kebijakan Keamanan Informasi apakah sudah terkontrol oleh prosedur dan kebijakan sesuai SMKI?
B. Potensi 3rd party (Vendor, Rekanan, Supplier) tidak menerapkan kebijakan Keamanan Informasi apakah sudah terkontrol oleh prosedur dan kebijakan sesuai SMKI?
C. Resiko Keamanan Informasi pada saat work from remote atau work from home (WFH), apakah sudah terkontrol oleh prosedur dan kebijakan sesuai SMKI?

Pemetaan Terhadap Annex.A (*document control*) ISO/IEC 27001:2013

Tabel 1. Pemetaan Terhadap Annex/ Dokumen Kontrol ISO/IEC 27001:2013

Pemetaan Terhadap Klausa ISO/IEC 27001:2013

Tabel 2. Pemetaan terhadap Klausa ISO/IEC 27001:2013

Klausa	Deskripsi	Detail Deskripsi	Checklist	Sesuai	Tidak	Catatan	Relasi Rumusan Masalah
4	**Konteks Organisasi**						
4.4	Sistem manajemen keamanan informasi	Organisasi harus menetapkan dan memelihara, terus meningkatkan SMKI sesuai dg persyaratan standar ini	Apa saja yg menjadi supporting process dan improvement process dalam keseluruhan process ini	√		Sesuai kebijakan internal BRI (dalam aturan dan panduan operasional)	A. Karyawan Baru
			Apakah terdapat dokumentasi terkait proses yg dijalankan oleh organisasi	√			
5	**Kebijakan**						
5.2	Peraturan dan kebijakan	Top manajemen harus menetapkan kebijakan keamanan informasi dan sesuai dg tujuan organisasi	Apakah organisasi telah menentukan kebijakan keamanan informasi?	√		Sesuai kebijakan internal BRI (informasi dan kewenangan serta arahan di distribusikan sesuai keburuhan masing-masing unit kerja)	A. Karyawan Baru B. Rekanan & Supplier
			Apakah kebijakan yg dibuat sudah sesuai dg tujuan organisasi	√			
			Apakah kebijakan dikomunikasikan ke seluruh organisasi dan pihak berkepentingan?	√			
			Apakah kebijakan keamanan informasi di dokumentasikan?	√			
6	**Perencanaan**						
6.1	Tindakan untuk menangani risiko keamanan informasi	Organisasi perlu mengidentifikasi resiko dan peluang yang mungkin timbul dari setiap aktivitas dan menentukan action plan atau tindakan untuk mengatasinya	Apakah terdpat kebijakan untuk prosedur terkait tindakan untuk menangani resiko keamanan informasi?	√		Sesuai kebijakan internal BRI (prosedur mitigasi serta penanganan terhadap resiko yang telah di identifikasi dan di analisa inherent risk maupun non inherent)	B. Rekanan & Supplier C. Kebijakan Akses WFH
			Apakah metode yang digunakan untuk menganalisa resiko?	√			
7	**Pendukung**						
7.3	Kepedulian	Organisasi memastikan bahwa setiap orang mengetahui dan sadar akan kebijakan keamanan informasi	Apakah organisasi melakukan awareness dan sosialisasi untuk karyawan mengenai keamanan informasi?	√		Sesuai kebijakan internal BRI (Sosialisasi dan broadcast rutin, E-learning wajib, meeting dalam doa pagi)	A. Karyawan Baru
			Apakah awareness dilakukan untuk pegawai baru?	√			
			Apakah terdpat program awareness mengenai keamanan informasi?	√			
8	**Operasi**						
8.1	perencanan dan pengendalian operasional	Organisasi harus mengendalikan perubahan yang direncanakan dan meninjau kensekwensi dari perubahan yang tidak di inginkan, mengambil tindakan untuk mengurangi efek samping yang diperlukan	Apakah seluruh bagian dalam organisasi sudah memiliki sop	√		Sesuai kebijakan internal BRI (panduan dan prosedur operasional yg disahkan serta di review berkala pada setiap departemen dan fungsi tiap divisi)	A. Karyawan Baru B. Rekanan & Supplier C. Kebijakan Akses WFH
9	**Evaluasi kinerja**						
9.1	Pemantauan, pengukuran, analisis dan evaluasi	Organisasi harus melakukan pemantauan, pengukuran , analisis dan evaluasi terkait dengan sistem manajemen keamanan informasi	Terkait implementasi sistem manajemen keamanan informasi, apa saja hal yg menjadi parameter pengukuran bagi organisasi?	√		Sesuai kebijakan internal BRI (metode pemantauan oleh fungsi quality assurance dengan pengamatan secara langsung, audit internal, meminta informasi dan evidence, terdokumentasi perbaikan jika ada atau saran untuk meningkatkan)	A. Karyawan Baru
			Apakah terdapat periode untuk melakukan pemantauan dan pengukuran?	√			
			Apakah terdapat metode yang di gunakan untuk pemantauan pengukuran analisis dan evaluasi?	√			
			Kapan pemantauan dan pengukuran harus dilakukan?	√			
			Siapa yang akan memantau dan mengukur?	√			
			Apakah terdapat dokumentasi terkait pemantauan dan pengukuran?	√			
10	**Peningkatan**						
10.2	Perbaikan berkelanjutan	Organisasi melakukan perbaikan berkelanjutan untuk menjaga efektifitas dari implementasi sistem manajemen keamanan informasi	Terkait dengan aspek perbaikan berkelanjutan, apa saja aktivitas yang sudah dilakukan oleh organisasi?	√		Sesuai kebijakan internal BRI (review berkala dan meningkatkan kepatuhan implementasi masing-masing bagian terkait SMKI, sosialisasi dan arahan)	B. Rekanan & Supplier C. Kebijakan Akses WFH
			Seberapa efektif aktivitas tersebut dalam upaya melakukan perbaikan berkelanjutan?	√			

Re-assessment Pelaksanaan Pada Bagian Komunikasi Satelit Monitoring

Untuk menilai konsistensi dari implementasi sesuai pemetaan kerangka SMKI sertifikasi yang telah didapat, digunakan system skoring dari data yang telah dikumpulkan selama kerja magang pada Fungsi Payload dan CSM terhadap kriteria yang ada agar dapat dengan mudah diketahui parameternya.

Tabel 3. Skoring Pada Permasalahan A: Resiko Karyawan Baru

No	Rumusan Masalah	Klausa & Annex	Deskripsi	Pelaksanaan		
				Dilaksanakan	Sering	Selalu
1	A	Klausa 4.4	Organisasi harus menetapkan dan memelihara, terus meningkatkan SMKI sesuai dg persyaratan standar ini (ISO/IEC 27001:2013)			1
2	A	Klausa 5.2	Top manajemen harus menetapkan kebijakan keamanan informasi dan sesuai dg tujuan organisasi			1
3	A	Klausa 7.3	Organisasi memastikan bahwa setiap orang mengetahui dan sadar akan kebijakan keamanan informasi			1
4	A	Klausa 8.1	Organisasi harus mengendalikan perubahan yang direncanakan dan meninjau konsekwensi dari perubahan yang tidak di inginkan, mengambil tindakan untuk mengurangi efek samping yang diperlukan			1
5	A	Klausa 9.1	Organisasi harus melakukan pemantauan, pengukuran , analisis dan evaluasi terkait dengan sistem manajemen keamanan informasi			1
6	A	Annex 5.1.1	Penyusunan berbagai kebijakan keamanan informasi baik untuk high level maupun low level. Kebijakan tersebut juga disetujui, dipublikasikan, dan dikomunikasikan ke pegawai dan pihak terkait lainya		1	
7	A	Annex 7.1.2	Pemberian informasi mengenai prosedur dan kebijakan untuk pegawai			1
8	A	Annex 7.2.2	Pemberian kepedulian (awarenes), pendidikan, dan pelatihan keamanan informasi kepada seluruh pegawai atau pihak ketiga di organisasi		1	
9	A	Annex 9.2.1	Implementasi proses registrasi dan de-registrasi pengguna			1
10	A	Annex 9.2.4	Implementasi proses pengalokasian informasi otentifikasi rahasia pengguna			1
11	A	Annex 9.2.5	Review terhadap hak akses pengguna pada jangka waktu tertentu	1		
12	A	Annex 10.1.2	Kebijakan penggunaan pelindungan dan masa hidup kunci kriptografi harus di kembangkan dan di implementasikan dalam keseluruhan siklus			1
13	A	Annex 11.1.3	Implementasi kebijakan keamanan mulai dari saat masuk			1
14	A	Annex 11.2.6	Implementasi panduan pengamanan peralatan dan aset yang digunakan di luar kantor			1
15	A	Annex 11.2.9	Implementasi kebijakan clear desk dan clear screen			1
16	A	Annex 12.2.1	Implementasi panduan perlindungan terhadap malware			1
17	A	Annex 12.5.1	Implementasi prosedur instalasi software pada sistem operasional			1
18	A	Annex 13.2.4	Implementasi NDA			1
19	A	Annex 16.1.5	Proses respon terhadap setiap insiden keamanan informasi yang terjadi			1
20	A	Annex 17.1.3	Organisasi harus memeriksa kendali keberlangsungan keamanan informasi yang di tetapkan dan di implementasikan secara berkala		1	
21	A	Annex 18.2.3	Pelaksanaan review terhadap kesesuaian teknis sistem informasi sesuai kebijakan dan standar organisasi			1
Total Score				**1**	**3**	**17**
Prosentase				**5%**	**14%**	**81%**

Tabel 4. Skoring Pada Permasalahan B: Resiko Pihak Ketiga (Rekanan, Vendor, Supplier)

No	Rumusan Masalah	Klausa & Annex	Deskripsi	Pelaksanaan		
				Dilaksanakan	Sering	Selalu
1	B	Klausa 5.2	Top manajemen harus menetapkan kebijakan keamanan informasi dan sesuai dg tujuan organisasi			1
2	B	Klausa 6.1	Organisasi perlu mengidentifikasi resiko dan peluang yang mungkin timbul dari setiap aktivitas dan menentukan action plan atau tindakan untuk mengatasinya			1
3	B	Klausa 8.1	Organisasi harus mengendalikan perubahan yang direncanakan dan meninjau konsekwensi dari perubahan yang tidak di inginkan, mengambil tindakan untuk mengurangi efek samping yang diperlukan			1
4	B	Klausa 10.2	Organisasi melakukan perbaikan berkelanjutan untuk menjaga efektifitas dari implementasi sistem manajemen keamanan informasi			1
5	B	Annex 7.1.2	Pemberian informasi mengenai prosedur dan kebijakan untuk pegawai			1
6	B	Annex 7.2.2	Pemberian kepedulian (awarenes), pendidikan, dan pelatihan keamanan informasi kepada seluruh pegawai atau pihak ketiga di organisasi		1	
7	B	Annex 11.1.3	Implementasi kebijakan keamanan mulai dari saat masuk			1
8	B	Annex 12.5.1	Implementasi prosedur instalasi software pada sistem operasional			1
9	B	Annex 13.2.4	Implementasi NDA			1
10	B	Annex 15.1.3	Perjanjian dengan pemasok harus termasuk persyaratan untuk mengatasi resiko keamanan informasi terkait rantai pasok layanan dan produk teknologi informasi			1
Total Score			**0**	**0**	**1**	**9**
Prosentase			**0%**	**0%**	**10%**	**90%**

Tabel 5. Skoring pada permasalahan C: Resiko Work From Home / WFH Terkait Pembatasan Saat Pandemi

No	Rumusan Masalah	Klausa & Annex	Deskripsi	Pelaksanaan		
				Dilaksanakan	Sering	Selalu
1	C	Klausa 6.1	Organisasi perlu mengidentifikasi resiko dan peluang yang mungkin timbul dari setiap aktivitas dan menentukan action plan atau tindakan untuk mengatasinya			1
2	C	Klausa 8.1	Organisasi harus mengendalikan perubahan yang direncanakan dan meninjau konsekwensi dari perubahan yang tidak di inginkan, mengambil tindakan untuk			1
3	C	Klausa 10.2	Organisasi melakukan perbaikan berkelanjutan untuk menjaga efektifitas dari implementasi sistem manajemen keamanan informasi			1
4	C	Annex 5.1.1	Penyusunan berbagai kebijakan keamanan informasi baik untuk high level maupun low level. Kebijakan tersebut juga disetujui, dipublikasikan, dan dikomunikasikan ke pegawai dan pihak terkait lainya		1	
5	C	Annex 6.1.1	Penetapan dan pengalokasian tanggungjawab terkait keamanan informasi			1
6	C	Annex 6.2.1	Penyusunan kebijakan perangkat mobile dan kemanan informasi pendukung			1
7	C	Annex 8.2.1	Klasifikasi informasi berdasarkan ketentuan hukum, value, critically, dan sensitivitas terhadap disclosure atau modifikasi yang tidak terotorisasi			1
8	C	Annex 9.2.1	Implementasi proses registrasi dan de-registrasi pengguna			1
9	C	Annex 9.2.4	Implementasi proses pengalokasian informasi otentifikasi rahasia pengguna			1
10	C	Annex 9.2.5	Review terhadap hak akses pengguna pada jangka waktu tertentu	1		
11	C	Annex 10.1.2	Kebijakan penggunaan pelindungan dan masa hidup kunci kriptografi harus di kembangkan dan di implementasikan dalam keseluruhan siklus			1
12	C	Annex 11.2.6	Implementasi panduan pengamanan peralatan dan aset yang digunakan di luar kantor			1
13	C	Annex 11.2.9	Implementasi kebijakan clear desk dan clear screen			1
14	C	Annex 12.2.1	Implementasi panduan perlindungan terhadap malware			1
15	C	Annex 14.1.2	Informasi yang terdapat dalam layanan aplikasi yang melewati jaringan publik harus dilindungi dari aktivitas yang bersifat menipu, perselisihan kontrak, dan pembukaan rahasia yang tidak sah, duplikasi atau balasan pesan yang tidak sah			1
16	C	Annex 17.1.3	Organisasi harus memeriksa kendali keberlangsungan keamanan informasi yang di tetapkan dan di implementasikan secara berkala		1	
17	C	Annex 18.2.3	Pelaksanaan review terhadap kesesuaian teknis sistem informasi sesuai kebijakan dan standar organisasi			1
Total Score			**1**	**1**	**2**	**14**
Prosentase			**6%**	**6%**	**12%**	**82%**

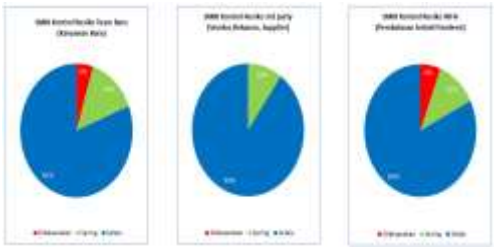
Analisis (Evaluasi)

Dalam penilaian konsistensi pelaksanaan terhadap klausa dan dokumen control SMKI berbasis ISO/IEC 27001:2013 pada Bagian Komunikasi Satelit Monitoring, parameter **"Dilaksanakan"** artinya hal tersebut sudah diatur pada prosedur dan kebijakan organisasi serta dijalankan tapi tidak selalu sebab terkait dengan wewenang, bagian atau fungsi lain dalam satu korporasi tidak dalam control internal. Sedangkan parameter **"Sering"** merupakan hal yang pelaksanaan pada internal Bagian Komunikasi Satelit Monitoring sudah biasa dilaksanakan secara internal tapi tidak menjadi prosedur baku dikarenakan sudah ada pelaksanaan yang wajib dan baku dari perusahaan secara keseluruhan. Dan yang terakhir adalah parameter **"Selalu"** Adalah hal wajib penanganan terkait kelola data, informasi, serta dokumen maupun prosedur yang sudah selalu tekankan dan dilaksanakan serta menjadi pedoman dalam operasional.

Disamping parameter tersebut diatas, kriteria yang dipergunakan untuk menilai adalah sebagai berikut :

- Sesuai Sempurna > **90% s/d 100%**
- Konsisten Sesuai > **80% s/d 90%**
- Kurang Sesuai > **70% s/d 80%**
- Tidak memenuhi Syarat < **70%**

Berdasarkan table checklist yang berisi mapping klausa dan dokumen kontrol terhadap kebijaksanaan manajemen, pemahaman stake holder (Bagian Komunikasi Satelit Monitoring), pelaksanaan, kepatuhan, dan BPO (Buku Panduan Operasional), didapatkan hasil scoring:



Gambar 9. Diagram Penilaian Konsistensi Penerapan Klausa dan Dokumen Kontrol ISO/IEC 27001:2013

- **81%** untuk kontrol resiko Team atau Karyawan Baru
- **90%** untuk kontrol resiko Pihak Ketiga
- **82%** untuk kontrol resiko Work From Home (WFH)

5. KESIMPULAN

Dari analisa data yang telah didapat maka bisa diketahui konsistensi pelaksanaan penerapan klausa, dokumen kontrol sertifikasi ISO 27001:2013 (*ISMS*), serta kebijakan yang telah di terapkan dan dijadikan pedoman seluruh stakeholder Bagian Komunikasi Satelit Monitoring (Manager, Engineer, Operator) mendapatkan kriteria nilai yang tinggi.

Sehingga dapat ditarik kesimpulan bahwa seluruh team telah memahami hak serta kewajiban nya dan melaksanakan secara konsisten dengan bertanggungjawab dalam menjaga keamanan informasi sesuai dengan kerangka sistem manajemen keamanan informasi (SMKI).

DAFTAR PUSTAKA

R. Sarno and I. Iffano, (2009). Sistem Manajemen Keamanan Informasi, 1st ed. Surabaya: ITS Press.

Brunner, M. Sauerwein, C. Felderer, M. Breu, R. (2020). Risk management practices in information security: Exploring the status quo in the DACH region. Journal & Books Science Direct Elsevier, Vol 92, 102776

Tata Kelola Teknologi Informasi: Cara untuk menyelaraskan Strategy IT dan Proses Bisnis. Pada Maret 2021 diakses dari https://itgid.org/tata-kelola-teknologi-informasi-cara-untuk-menyelaraskan-strategi-it-dan-proses-bisnis

Peraturan Menteri BUMN PER-02/MBU/2013: Panduan Penyusunan Pengelolaan Teknologi Informasi Badan Usaha Milik Negara. (2013, Februari) diakses dari https://jdih.bumn.go.id/lihat/PER-02/MBU/2013

ISO/IEC 27001 : Information Security Management. Pada Mei 2021 diakses dari https://www.iso.org/isoiec-27001-information-security.html

ISO/IEC_27001. Pada Mei 2021 diakses dari https://en.wikipedia.org/wiki/ISO/IEC_27001

Knowledge. Pada Juni 2021 diakses dari https://www.robere.co.id/posts/1/knowledge/en

Informasi Perusahaan. Pada Juni 2021 diakses dari https://bri.co.id/info-perusahaan