Journal of Applied Informatics and Computing
(JAIC) Vol.x, No.1, Juli 2024, pp. 01~11
e-ISSN: 2548-6861

Analisis Sistem Keamanan Akses Fisik Ruang Perangkat Next Generation Network Berdasarkan Standar SNI 8799 Tahun 2019 PT.Telkom Indonesia

Mhd.Rafidrahman[1]*, Andy Triwinarko[2]**
* Teknik Informatika, Politeknik Negeri Batam
** Rekayasa Keamanan Siber, Politeknik Negeri Batam
mhd.rafid.4332011002@students.polibatam.ac.id[1] , andy@polibatam.ac.id[2]

Article Info

Article history:
Received 2024 - 06 - 28
Revised 2024 - 07 - 01
Accepted …

Keyword:
Next generation network,
SNI 8799,
Keamanan informasi,
Keamanan fisik.

ABSTRACT

Physical security of *Next Generation Network (NGN)* equipment rooms at PT Telkom Indonesia is crucial to maintain the integrity and reliability of the national telecommunications network. This study aims to analyze the current level of physical access security, observe the conditions of *NGN* equipment rooms, and propose improvements in accordance with the SNI 8799:2019 security standards. Through analysis and observation methodologies, it was found that while the existing physical security systems adequately protect most areas, there are vulnerabilities that need immediate attention. One such issue is the use of conventional keys at access points, which are inadequate, along with the need to increase the number of *CCTV* cameras to monitor critical areas more effectively. Recommended improvements include enhancing security systems with biometric technology for tighter access control, augmenting surveillance infrastructure such as *CCTV*, and implementing comprehensive standard regulations to ensure compliance with physical security arrangements. These steps are expected to enhance protection of *NGN* equipment from physical threats, ensuring optimal system performance for PT Telkom Indonesia in delivering reliable and secure telecommunications services.

This is an open access article under the CC–BY-SA license.

I. PENDAHULUAN

Dengan kemajuan teknologi yang semakin pesat pada era ini, Teknologi Informasi (TI) telah menjadi faktor krusial dalam memenuhi kebutuhan perusahaan. PT. Telkom Indonesia, sebagai penyedia layanan telekomunikasi dan datacenter, memiliki kontrol akses terhadap monitoring jaringan fiber optik di beberapa wilayah Indonesia. TI dianggap mampu memberikan solusi untuk berbagai proses bisnis perusahaan. Seiring dengan pertumbuhan yang cepat dari penggunaan teknologi informasi, kebutuhan akan jaringan telekomunikasi juga semakin meningkat, dan ruang *Next Generation Network* hadir sebagai penyedia manajemen jaringan telekomunikasi yang disalurkan kepada pengguna. Hal ini mencakup perlindungan fisik terhadap peralatan dan teknologi, termasuk penyimpanan data, server, perangkat telekomunikasi[1].

Ruang *Next Generation Network (NGN)* adalah ruang yang mengelola jaringan berbasis paket yang mampu menyediakan berbagai layanan telekomunikasi, dapat mengintegrasikan teknologi *broadband* dan *narrowband,* menyediakan *QoS (Quality of Service),*memiliki layer aplikasi yang independent terhadap layer transport, memungkinkan akses tanpa batas ke berbagai penyedia layanan dan mendukung mobilitas untuk menyediakan layanan di mana saja dan kapan saja bagi pengguna [2]. Mencakup perlindungan terhadap ruang perangkat telekomunikasi *next generation network* dibutuhkan adanya kontrol keamanan berdasarkan standar SNI 8799:2019.

Standar Nasional Indonesia (SNI) 8799-1 berisi panduan teknis untuk pusat data dalam bidang teknologi informasi,

JAIC e-ISSN: 2548-6861

yang diadopsi dari standar internasional ISO, *Uptime*, dan TIA-942, yang telah disesuaikan dengan kondisi di Indonesia[3]. SNI 8799-1 diterbitkan oleh Badan Standardisasi Nasional *(BSN)*. Standar ini menjadi syarat yang harus dipenuhi oleh berbagai lembaga yang ingin memiliki pusat data yang sesuai dengan standar nasional [4]. Pusat data untuk *next generation network* berperan penting dalam mendukung infrastruktur teknologi untuk ekosistem digital di Indonesia. Dalam konteks ini, penting untuk menganalisis penerapan SNI 8799:2019 terhadap ruang perangkat *next generation network*. Dengan melakukan analisis dan penerapan ini, dapat dipastikan bahwa praktik keamanan informasi yang diterapkan sesuai dengan standar nasional dan memberikan perlindungan optimal terhadap data sensitif yang dikelola. Tujuan penelitian ini adalah untuk melakukan analisis terhadap keamanan akses fisik pada ruang perangkat *next generation network*, serta memberikan rekomendasi berdasarkan hasil analisis tersebut. Berdasarkan observasi, wawancara, dan dokumentasi terhadap temuan gap yang dilakukan dengan PT. Telkom Indonesia, saat ini keamanan akses fisik di ruang *next generation network* masih kurang optimal dan belum sepenuhnya mematuhi standar keamanan fisik SNI 8799:2019. Sebagai solusi, peneliti menyarankan untuk melakukan analisis dan perancangan keamanan fisik yang mengacu pada standar tersebut.

A. Tinjauan Pustaka

1. Peneliti sebelumnya yang dilakukan oleh Salman nuzuli pada tahun 2020 dengan judul "Analisis Dan Perancangan Keamanan Fisik Data Center Berdasarkan Standar TIA-942 menggunakan *PPDIOO Life-cycle Approach* di pemerintahan Kabupaten Bandung Barat". Dalam penelitian ini, penulis meganalisa dan membuat perancangan keamanan fiisik pada pusat data center dengan menggunakan standar Tia-942 sebagai panduan analisis dan rancangan pada pusat data[5].
2. Peneliti sebelumnya yang dilakukan oleh faza ainun nafisah pada tahun 2020 dengan judul "Evaluasi keamanan informasi Data center berdasarkan standar ISO 27001:2013". Dalam penelitian ini, penulis melakukan evaluasi keamanan informasi data center dengan metode penelitian setudi kasus pada PT.Pupuk Kalimantan timur[6].
3. Peneliti sebelumnya yang dilakukan oleh Musthofa kamal pada tahun 2019 dengan judul "Perancangan sistem keamanan fisik pada Data center Cv.Media smart dengan menggunakan metode *NDLC* dengan berdasarkan standar TIA-942". Dalam penelitian ini, penulis melakukan perancangan sistem keamanan fisik dengan berdasarkan standar TIA-942[7].
4. Peneliti sebelumnya yang dilakukan oleh Digky,, B,P, & Endang, S,A pada tahun 2016 dengan judul "Analisis penerapan sistem keamanan fisik pada data center untuk melindungi data organisasi". Dalam penelitian ini, penulis melakukan analisis terkait dengan penerapan sistem keamanan fisik pada data center dengan berdasarkan standar BS ISO/IEC 17799[8].

B. Standar SNI 8799

SNI 8799:2019 pusat data, standarisasi dibagi kedalam 3 bagian, dokumen ini berlaku sebagai acuan pelaksanaan sertifikasi pusat data dengan lingkup SNI sebagai berikut [9].

Tabel 1.1 Pedoman Standar SNI 8799

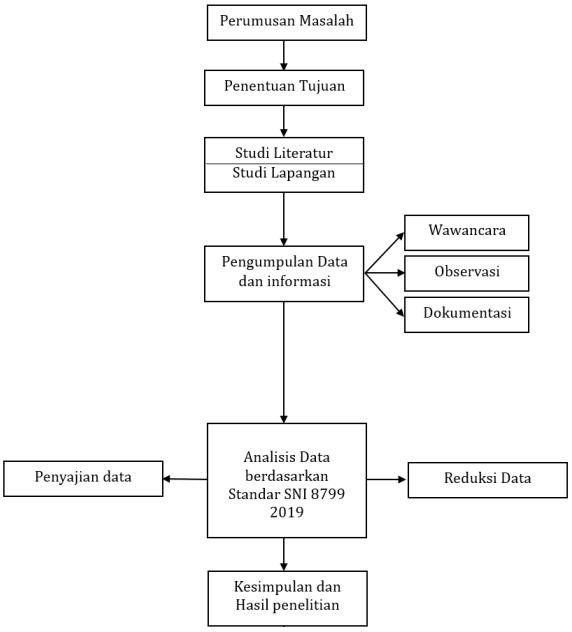
Katergori Panduan SNI		Tingkatan Level Pusat Data			
Bagian 1	: Panduan Spesifikasi teknis pusat data	STRATA 1	STRATA 2	STRATA 3	STRATA 4
Bagian 2	: Panduan Managmen Pusat data				
Bagian 3	: Panduan Audit pusat data				

1. Bagian 1 dari panduan ini berisi semua spesifikasi teknis yang diperlukan untuk merancang, membangun, dan mengoperasikan pusat data sesuai dengan standar SNI 8799:2019. Ini meliputi persyaratan untuk infrastruktur fisik seperti ruang server, sistem pendinginan, dan kebutuhan daya listrik. Selain itu, panduan ini juga mungkin mencakup spesifikasi untuk perangkat keras dan perangkat lunak yang digunakan dalam pusat data, serta aspek keamanan.
2. Bagian 2 dari panduan ini menyediakan arahan mengenai praktik manajemen yang efektif untuk operasional harian dan strategis pusat data sesuai dengan standar SNI 8799:2019. Ini termasuk prosedur untuk memonitor kesehatan sistem, manajemen kapasitas, manajemen perubahan, dan pemulihan dari bencana. Panduan ini juga dapat mencakup strategi untuk mengelola siklus hidup perangkat keras dan perangkat lunak dalam pusat data guna meningkatkan ketersediaan dan efisiensi secara maksimal.
3. Bagian 3 dari panduan ini memberikan penjelasan mengenai proses audit yang diperlukan untuk memverifikasi bahwa pusat data memenuhi semua persyaratan yang diatur dalam SNI 8799:2019. Audit ini mencakup evaluasi terhadap keamanan fisik, kehandalan sistem, ketersediaan layanan, serta kepatuhan terhadap kebijakan dan regulasi yang berlaku.

Panduan audit juga dapat mencakup langkah-langkah untuk melakukan audit internal secara rutin dan strategi menghadapi audit eksternal guna memastikan kepatuhan pusat data terhadap standar yang telah ditetapkan.

II. METODE

Metode Penelitian adalah prosedur yang digunakan untuk mengumpulkan data dan informasi yang nantinya akan diolah, dikembangkan, atau dianalisis secara ilmiah oleh peneliti. Penelitian ini fokus pada analisis keamanan akses fisik pada ruang perangkat *Next Generation Network* dengan standar SNI 8799:2019, menggunakan pendekatan kualitatif. Penelitian kualitatif ini bersifat deskriptif dan memanfaatkan analisis, dengan mengeksplorasi sudut pandang partisipan melalui strategi interaktif dan fleksibel. Proses pengumpulan dan pengolahan data mengikuti langkah-langkah yang didefinisikan, termasuk pendekatan analisis data kualitatif secara terus-menerus, sebagaimana disarankan oleh *Miles & Huberman (1984).* Metode ini merupakan pendekatan sistematis yang sering digunakan untuk memahami fenomena kompleks dalam konteks penelitian sosial dan ilmu pengetahuan lainnya. Dalam konteks penelitian ini di PT Telkom Indonesia, pendekatan ini diterapkan untuk mendalami aspek keamanan akses fisik pada perangkat *Next Generation Network* dengan cara yang terstruktur dan mendalam.



Gambar 2.1 *Metode Penelitian*

A. Perumusan Masalah

Pada penelitian kali ini penulisan mengambil topik analisis keamanan fisik pada Ruang Perangkat *Next Generation Network* pada PT.Telkom indonesia sebagai objek penelitian dengan menggunakan acuan standar SNI 8799:2019.

B. Penentuan Tujuan

Sesuai dengan analisis rumusan masalah maka dapat ditentukan tujuan dari penelitian ini.yang bertujuan untuk menganalisis Tingkat keamanan akses fisik pada ruang perangkat *Next Generation Network* di PT.Telkom indonesia. Dengan berdasarkan standar SNI 8799 Tahun 2019. Penelitian ini akan menyajikan rekomendasi perbaikan atau peningkatan untuk sistem keamanan fisik, seperti pengawasan kamera, sistem kunci pintu, atau sensor keamanan lainnya.

C. Studi Literatur

Pada tahap ini peneliti mempelajari sumber-sumber penelitian terkait untuk menelaah hubungan masalah yang akan dipecahkan dengan menggunakan literature dari jurnal-jurnal maupun media elektronik lainnya, yang berkaitan dengan analisis keamanan akses fisik dengan standar yang menjadi acuan bagi analisis keamanan fisik pada pusat data.

D. Studi Lapangan

Analisis data pada umumya membutuhkan setudi literature atau penelitian sebelumnya sebagai acuan atau pedoman dalam melakukan penelitian pada studi lapangan.

E. Pengumpulan Data (Data Collection)

Pengumpulan data di lapangan tentu berkaitan dengan teknik penggalian data, dan ia berkaitan pula dengan sumber dan jenis data, setidaknya sumber data dalam penelitian kualitatif berupa: (1) kata-kata dan (2) tindakan, selebihnya adalah data tambahan seperti dokumen atau sumber data tertulis, foto, dan statistik. [11]. Kata-kata dan tindakan orang-orang yang diamati atau diwawancarai merupakan sumber data utama. Sumber data utama dicatat melalui catatan tertulis atau melalui perekaman video, pengambilan foto, atau film.

F. Penyajian data (Data Display)

Yaitu susunan sekumpulan informasi yang memungkinkan penarikan kesimpulan dan pengambilan tindakan.

G. Reduksi Data (Data reduction).

Yaitu Data yang dikelompokkan selanjutnya disusun dalam bentuk narasi- narasi,sehingga berbentuk rangkaian informasi yang bermakna sesuai dengan masalah penelitian.

JAIC e-ISSN: 2548-6861

H. Penarikan kesimpulan

(Conclusion verivications) dimana kesimpulan tersebut diverivikasi selama proses penelitian. Verifikasi tersebut berupa tinjauan atau pemikiran kembali pada catatan lapangan yang mungkin berlangsung sekilas atau malah dilakukan secara seksama dan memakan waktu lama, serta bertukar pikiran. Sehingga makna-makna yang muncul dari data harus diuji kebenarannya, kekokohannya, dan kecocokannya sehingga membentuk validitasnya.

III. HASIL DAN PEMBAHASAN

Hasil dan pembahasan merupakan poin fokus utama dalam penelitian ini, dengan data yang dihimpun melalui empat metode utama pengumpulan informasi, termasuk wawancara, observasi, dan dokumentasi.

A. Deskripsi Penerapan sistem keamanan fisik pada Ruang Next Generation Network.

Salah satu kontrol dalam keamanan fisik yang diterapkan di PT. Telkom Indonesia adalah Administrative Controls. Kontrol ini dipimpin oleh manajemen untuk mengatur prosedur yang bertujuan untuk meminimalisir ancaman dan dampak kerusakan fisik pada pusat data. Di PT. Telkom Indonesia, *Section NOC (Network Operation Center)* bertanggung jawab sebagai pelaksana kontrol area *Next Generation Network*. *Section* ini terdiri dari 4 pegawai tetap dan 8 pegawai kontrak. *NOC* tidak hanya bertugas untuk meningkatkan kualitas dan kewaspadaan di ruang *Next Generation Network*, tetapi juga menyediakan pelatihan kepada anggota setiap section, termasuk *NOC*. Salah satu contoh pelatihan yang pernah dilakukan adalah pelatihan tentang pemadam kebakaran.

Prosedur dan kebijakan berperan penting dalam mengurangi risiko keamanan di Pusat Data *Next Generation Network*. Prosedur ini termasuk pengaturan akses yang ketat ke ruang *Next Generation Network*. Sebelum diizinkan masuk, pengunjung harus mendapatkan izin resmi dari rektorat, yang kemudian akan diteruskan kepada Kepala Section *NOC*. *NOC* mendampingi pengunjung ke ruangan Pusat Data *Next Generation Network*. Selama berada di ruang *Next Generation Network*, pengunjung harus mematuhi prosedur dan kebijakan yang telah ditetapkan oleh *NOC*.

Prosedur lain meliputi larangan bagi pegawai *NOC* untuk makan, minum, atau merokok di lingkungan Pusat Data *Next Generation Network*, serta kewajiban mereka untuk selalu mengunci ruangan saat tidak ada pegawai di dalamnya. Kebersihan ruangan *Next Generation Network* juga dijaga melalui prosedur dan kebijakan perawatan fasilitas pusat data. Pembersihan fasilitas ruangan *Next Generation Network* dilakukan secara teratur oleh staf dari *Network Operation Center (NOC)* atau *Network Area*, dibantu oleh petugas kebersihan di area tertentu. Dalam analisis terhadap ruang *Next Generation Network*, PT. Telkom Indonesia belum sepenuhnya menerapkan prosedur dan kebijakan terkait standarisasi untuk ruang Telekomunikasi *Next Generation Network*. Standarisasi diperlukan dalam pusat data telekomunikasi untuk memastikan penggunaan protokol, spesifikasi, dan prosedur yang telah ditetapkan guna menjamin interoperabilitas, keamanan, dan kinerja yang optimal dalam infrastruktur telekomunikasi. Ini mencakup aspek seperti protokol komunikasi, kabel dan konektivitas, keamanan data, manajemen energi, penyimpanan data, dan pemantauan infrastruktur.

Dengan mematuhi standar yang ditetapkan, pusat data dapat beroperasi dengan efisiensi tinggi, meningkatkan ketersediaan layanan, dan menjaga keamanan data yang disimpan dan ditransmisikan di dalamnya. Saat ini, ruang *NGN* telah mengimplementasikan beberapa tahapan dalam prosedur keamanan dan kebijakan, namun belum secara eksplisit mengadopsi standarisasi internasional atau nasional sebagai panduan yang pasti. Kontrol dalam keamanan fisik selanjutnya adalah *Physical Control* dan *Technical Controls* yang merupakan kontrol pengendalian keamanan ruang perangkat *Next generation network* dengan melakukan pencegahan maupun pengawasan dengan parameter fisik dan teknikal.

Alat keamanan fisik sebagai lapisan terluar adalah pagar, pagar berfungsi sebagai pemisah antara lokasi yang ingin dilindungi dengan lingkungan disekitarnya, ruangan *Next generation network* pada PT.Telkom indonesia bukitdangas sekupang,Batam berada pada gedung utama yang tergabung pada ruangan control, Ruang staff *NOC*, mushola, canteen, ruang dingset & ruang ups.

Ruang ruang tersebut tergabung dalam 1 Gedung yang dibatasi persetiap ruangan, yang mana area ruang ruang tersebut sudah dilengkapi *cctv*, *access door lock* dan Apar(Alat Pemadam Api Ringan). Gedung pada PT.Telkom indonesi pada umumnya sudah di keliligi oleh pagar yang mengitarinya sebagai batasan akses. Pagar ini merupakan lapisan terluar bagi lapisan keamanan gedung milik PT.Telkom Indonesia. Terdapat 1 pos keamanan pada pintu masuk gedung PT.Telkom indonesia, Gedung hanya memiliki 1 pos keamanan, dimana area PT.Telkom indonesia terdapat di area yang cukup jauh dari tempat tinggal penduduk, dan gedungnya terdapat pada area perbukita tanpa adanya tempat tinggal penduduk di sekitarnya.

PT.Telkom indonesia memiliki 5 Tenaga keamanan yang terbagi menjadi 2 shift dalam sehari, masing-masing shift bekerja selama 7 jam, tenaga keamanan ditempatkan pada pos jaga yang terletak digerbang utama masuk perusahaan. Tindakan pengamanan yang dilakukan antara lain adalah melakukan patroli pada area gedung,

memeriksa pintu dan jendela gedung atau bangunan pada zona yang menjadi tanggung jawab masing-masing. Ruang *Next generation network* berada di satu gedung yang berhubungan langsung dengan area gudang peralatan *NOC*, ruang *OTB* dan ruang *Electrical.* untuk menuju ke ruang *NGN* harus melewati 2 fase pintu, pintu pertama adalah pintu utama menuju ke ruang *utility OTB* atau *Optical Terminal Box* adalah perangkat infrastruktur jaringan telekomunikasi optik yang berfungsi sebagai titik terminasi bagi serat optik, pintu utama menuju ke ruang *Ngn* sudah diberikan fasilitas kunci pintu/gembok pada umumnya kunci ruang industry, dan di area didalam pintu utama sudah di lengkapi dengan 1 buah Kamera *CCTV* yang menghadap ke pintu 2 menuju ruang *Next generation network* dan 1 buah alat pemadam api ringan, pintu menuju ke ruang *NGN* selalu tertutup dan hannya pegawai *NOC* yang diberikan kewenangan untuk mengakses rung *Next generation network*. Pada pintu ke dua menuju ke ruang *NGN* sudah dilengkapi dengan fitur keamanan seperti *acess door lock code* & *Rfid*, namun sayangnya acess *door* tersebut tidak berfungsi/kondisi rusak, dan dilengkapi juga dengan dua alaram kebakaran.

Pada Area Pusat data Ruang *Next Generation Network*, sudah dilengkapi dengan fitur keamanan seperti 7 buah kamera *CCTV* yang mengarah ke setiap rak server telekomunikasi, 4 teknologi Air pemadam api *automatic*, 6 buah *Detecktor* Asap, dan 3 buah *AC* pendingin ruangan yang berkapasitas lebih dari 5pk yang bekerja terus selama 24 jam dengan suhu rata-rata 22.9 derajat *celcius, control* suhu ruangan ini sangat penting untuk menjaga suhu dan sirkulasi udara didalam ruangan agar server tidak mudah panas. Dan dilengkapi dengan 20 lampu *Led* sebagai penerang ruangan dan alaram kebakaran, dan sudah dilengkapi dengan lantai Raised floor, lantai yang ditinggikan, dimana area bawah antai yang ditinggikan digunaka sebagai jalur kabel *fiber optic* dan kabel *electrical* listrik.

Listrik untuk Pusat Data *NGN* dipasok oleh PLN (Perusahaan Listrik Negara). Untuk situasi darurat, ruang perangkat *Next Generation Network* dilengkapi dengan *UPS (Uninterruptible Power Supply)* sebagai cadangan listrik yang didukung oleh genset. Selain itu, untuk melindungi dari lonjakan tegangan akibat petir, beberapa sisi gedung telah dipasang penangkal petir. Untuk mitigasi risiko kebakaran, PT. Telkom Indonesia telah menempatkan hand extinguisher di area pos keamanan yang berdekatan dengan pintu gerbang utama.

B. Analisa Penerapan Sistem Keamanan Fisik pada Ruang Next Generation Network

Analisis sistem keamanan fisik di ruang *Next Generation Network* PT. Telkom Indonesia ini dilakukan dengan menggunakan referensi dan landasan teori yang diuraikan pada Bab II, yaitu Standar Nasional Indonesia (SNI) 8799:2019 yang diterbitkan oleh Badan Standardisasi Nasional (BSN) pada tahun 2019. Standar ini mencakup praktik tentang panduan spesifikasi teknis, manajemen, dan audit pusat data. Setelah melakukan wawancara, observasi, dan dokumentasi, ditemukan beberapa kekurangan dalam ruang *Next Generation Network* berdasarkan evaluasi dengan menggunakan Standar SNI 8799:2019 sebagai berikut:

1) Regulasi standarisasi untuk ruang *Next Generation Network* belum tersedia secara spesifik karena ruang *NGN* di PT. Telkom Indonesia masih dalam tahap pengembangan. Berbagai alasan mengapa PT. Telkom Indonesia belum sepenuhnya menerapkan standar SNI 8799 pada ruang *NGN* termasuk keterbatasan sumberdaya seperti waktu, tenaga, dan finansial; kepatuhan terhadap standar lain yang relevan; kompleksitas infrastruktur yang ada; proses internal pembaharuan dan evaluasi; serta evolusi teknologi dan keamanan yang terus berubah. Perusahaan perlu merencanakan penerapan standar secara bertahap untuk memastikan keamanan fisik yang optimal di ruang *NGN* mereka.
2) Keterbatasan pelatihan dalam keamanan fisik menyebabkan karyawan PT. Telkom Indonesia memiliki pemahaman yang kurang mendalam tentang topik ini, meskipun mereka memiliki pemahaman dasar yang memadai secara umum. Saat ini, pelatihan hanya fokus pada pemadaman kebakaran di lingkungan perusahaan. PT. Telkom Indonesia merencanakan langkah-langkah untuk mengatasi masalah ini dengan mengembangkan program pelatihan khusus yang mencakup pemahaman mendalam tentang standar seperti SNI 8799, teknologi biometrik, pengelolaan *CCTV*, dan prosedur keamanan fisik lainnya. Mereka juga akan bekerjasama dengan lembaga pelatihan keamanan atau konsultan independen untuk bantuan dalam implementasi standar keamanan fisik, serta menghadirkan ahli keamanan untuk memberikan bimbingan langsung dan menunjukkan praktik terbaik kepada tim internal. Pembentukan tim khusus atau unit keamanan fisik direncanakan untuk meningkatkan keterampilan dan pengetahuan yang relevan, sambil melakukan evaluasi rutin untuk memastikan efektivitas program pelatihan dan implementasi keamanan fisik, serta mengidentifikasi area perbaikan.
3) Kebijakan *Vendor* dalam berkunjung ke ruang *Next Generation Network*, Kebijakan berkunjung ke Ruang *NGN* untuk tamu seperti *vendor* atau mitra dari PT.Telkom indonesia sedikit minim, dikarenakan terkadang *vendor* yang berkunjung ke ruang *NGN* seharusnya selalu di awasi oleh pihak *NOC*, namun setelah dilakukannya Observasi, vedor teradang jarang di awasi oleh pihak *NOC* disaat jam Lembur.

4) Kebijakan dalam mengkosumsi makanan, minuman, dan merokok di lingkungan Ruang Pusat data *NGN*, terdapat kebijakan untuk tidak makan, minum dan merokok di lingkungan Ruang *Next generation network*, namun wawancara yang dilakukan peneliti mengungkap bahwa pernah terjadi pegawai PT.Telkom indonesia membawa makanan dan minuman masuk ke ruang *NGN* ketika disaat jam kerja lembur.

5) Pegawai PT. Telkom Indonesia memberikan respon positif terhadap pelaksanaan kebijakan baru mengenai keamanan fisik berdasarkan standar SNI 8799. Mereka menganggap langkah ini penting untuk meningkatkan standar keamanan di ruang *Next Generation Network (NGN).* Dengan menerapkan standar ini, pegawai yakin bahwa keamanan fisik akan lebih terjaga dan risiko gangguan atau ancaman dapat diminimalkan. Mereka bersedia untuk menyesuaikan diri dengan perubahan ini dan berkomitmen mendukung upaya perusahaan dalam mencapai tingkat keamanan yang optimal sesuai dengan standar yang telah ditetapkan.

6) Kunci ruang Perangkat *Next generation network* (*NGN*) pada pintu pertama menuju ruang *Ngn*, dan ruang OTB (*Optical Terminal Box)* masih belum menggunakan kunci yang berteknologi seperti *Finjer print* atau *RFID*, dan *Biometric Control*, kunci ruang hanya menggunakan kunci konvensional yang mengandung beberapa resiko seperti kemungkinan untuk hilang dan mudah di gandakan atau di duplikat. Dan untuk kunci ruang ke dua yang menuju ke ruang *Next generation network*, sudah menggunakan kunci yang berteknologi seperti *Finjer Print* dan *access door Lock code*, namun setelah dilakukannya observasi dan penelitian GAP, kunci atau *acces door lock* tersebut sudah tidak digunakan lagi, karena Error atau rusak.

7) Efektivitas *CCTV* yang terpasang di Ruang Perangkat *NGN* sudah dilengkapi dengan 7 kamera *CCTV* yang mengarah ke setiap sisi rak server. Terdapat 1 kamera *CCTV* di pintu masuk kedua ruang *NGN*. Namun, setelah dilakukan observasi, terungkap bahwa tidak ada kamera *CCTV* yang terpasang di area pintu masuk pertama menuju ruang *NGN* dan *OTB*. PT.Telkom Indonesia berencana untuk meningkatkan sistem keamanan dengan menambah lebih banyak *CCTV* di area-area kritis di sekitar ruang *NGN*. Sebelum menambahkan kamera baru, mereka akan mengevaluasi kebutuhan, seperti lokasi pintu masuk, koridor utama, dan area dengan peralatan penting *NGN* yang rentan terhadap ancaman keamanan. Penambahan *CCTV* akan terintegrasi dengan sistem keamanan yang sudah ada, termasuk pengawasan manusia dan teknologi keamanan lainnya, untuk memaksimalkan efektivitas dan responsibilitas sistem keamanan secara keseluruhan. Dengan langkah ini, diharapkan PT. Telkom Indonesia dapat lebih baik dalam mengamankan ruang *NGN* mereka dari potensi ancaman fisik.

8) UPS (*Uninterruptible Power Supply)* , PT.Telkom indonesia sudah meyediakan daya cadangan listrik sementara jika terjadinya pemadaman listrik secara tiba–tiba dari *PLN*, dan dilakukannya *Observasi* pada ruang ups, perlunya ditingkatkan kembali kunci akses pintu pada ruang UPS.

C. Analisis GAP Ruang Next Generation Network.

Tabel 4.1 dan *Tabel 4.2* berikut ini menunjukkan hasil Gap kondisi keamanan fisik dan manajemen pusat data pada Ruang Perangkat *Next Generation Network* saat ini dengan acuan standar SNI 8799:2019.

Tabel 3.1 *Analisis GAP, Spesifikasi Teknis pusat data*

SPESIFIKASI TEKNIS PUSAT DATA													
SNI 8799		STRATA 1			STRATA 2			STRATA 3			STRATA 4		
No	Spesifikasi Teknis	Tinjauan Kebutuhan	Kondisi	Cross/ Check	Tinjauan Kebutuhan	Kondisi	Cross/ Check	Tinjauan Kebutuhan	Kondisi	Cross/ Check	Tinjauan Kebutuhan	Kondisi	Cross/ Check
1	Pemilihan Gedung												
1.1	Tidak berada pada area rentan bencana seperti yang dipetakan pada peta BMTG	Tidak dipersyaratkan	Area ruang ngn dan gedung berada pada area yang aman dari bencana	✕	Tidak dipersyaratkan	Area ruang ngn dan gedung berada pada area yang aman dari bencana	✕	Dipersyaratkan	Area Gedung dan area ruang Ngn berada pada area tidak rentan bencana dan aman.	✓	Dipersyaratkan	Area Gedung dan area ruang Ngn berada pada area tidak rentan bencana dan aman.	✓
2	Parkir Area Kendaraan												
2.1	Pemisahan area parkir karyawan dan pengunjung	Tidak dipersyaratkan	Area parkir masih tergabung menjadi 1 dengan pegawai	✓	Tidak dipersyaratkan	Area parkir masih tergabung menjadi 1 dengan pegawai	✓	Dipisahkan secara fisik dengan pagar	Area parkir belum dipisah antara pengujung dengan pegawai	✕	Dipisahkan secara fisik dengan pagar	Area parkir belum dipisah antara pengujung dengan pegawai	✕

3	**Persyaratan Catu daya listrik pusat data**												
3.1	Titik masuk listrik pertama	1 jalur primer	Hanya terdapat 1 jalur masuk arus listrik	✓	1 jalur primer	Hanya terdapat 1 jalur masuk arus listrik	✓	2 jalur primer, 1 aktif dan 1 siaga	Belum diterapkan	✗	2 jalur primer aktif	Belum diterapkan	✗
4	**Persyaratan Uninterruptible Power Supply (UPS)**												
4.1	Sambungan langsung otomatis	Tidak dipersyaratkan	Sudah diterapkan Jalur sendiri untuk ups	✗	Tidak harus jalur sendiri	Sudah diterapkan Jalur sendiri untuk ups	✗	Harus jalur sendiri	Sudah menerapkan jalur sendiri bagi ups	✓	Harus jalur sendiri	Sudah menerapkan jalur sendiri bagi ups	✓
4.2	Pengaturan perawatan sambungan langsung	Tidak dipersyaratkan	Sudah diterapkan Jalur sendiri untuk ups	✗	Tidak jalur sendiri yang menghubung kan ke output panel UPS	Sudah diterapkan Jalur sendiri untuk ups	✗	Jalur sendiri yang menghubung kan ke output panel UPS	Sudah menerapkan jalur sendiri bagi ups	✓	Jalur sendiri yang menghubung kan ke output panel UPS	Sudah menerapkan jalur sendiri bagi ups	✓
5	**Spesifikasi Sistem Pendingin**												
5.1	Temperatur ruangan : 18 derajat – 27 derajat celcius	Dipersyaratkan	Sudah diterapkan	✓	Dipersyaratkan	Sudah diterapkan	✓	Dipersyaratkan	Sudah diterapkan	✓	Dipersyaratkan	Sudah diterapkan	✓
5.2	Tingkat perubahan temperatur ruangan per-jam maksimum : 5 derajat Celcius	Dipersyaratkan	Sudah diterapkan	✓	Dipersyaratkan	Sudah diterapkan	✓	Dipersyaratkan	Sudah diterapkan	✓	Dipersyaratkan	Sudah diterapkan	✓
6	**Persyaratan Sistem jaringan pusat data**												
6.1	Memiliki label kabel yang terdiri dari nomor rak dan nomor baris pada rak	Dipersyaratkan	Sudah diterapkan penomoran dan pelabelan pada rak dan kabel	✗	Dipersyaratkan	Sudah diterapkan penomoran dan pelabelan pada rak dan kabel	✗	Dipersyaratkan	Sudah diterapkan penomoran dan pelabelan pada rak dan kabel	✗	Dipersyaratkan	Sudah diterapkan pelabelan setiap kabel, dan penomoran pada rak	✓
6.2	Tersedia jalur terpisah bagi penyedia layanan data komunikasi	Tidak dipersyaratkan	Sudah menerapkan traking kabel	✗	Dipersyaratkan	Sudah menerapkan traking kabel	✗	Dipersyaratkan	Sudah diterapkan jalur dan tracking	✓	Dipersyaratkan	Sudah diterapkan jalur dan tracking	✓
6	**Persyaratan Sistem jaringan pusat data**												
6.1	Memiliki label kabel yang terdiri dari nomor rak dan nomor baris pada rak	Dipersyaratkan	Sudah diterapkan penomoran dan pelabelan pada rak dan kabel	✗	Dipersyaratkan	Sudah diterapkan penomoran dan pelabelan pada rak dan kabel	✗	Dipersyaratkan	Sudah diterapkan penomoran dan pelabelan pada rak dan kabel	✗	Dipersyaratkan	Sudah diterapkan pelabelan setiap kabel, dan penomoran pada rak	✓
6.2	Tersedia jalur terpisah bagi penyedia layanan data komunikasi	Tidak dipersyaratkan	Sudah menerapkan traking kabel	✗	Dipersyaratkan	Sudah menerapkan traking kabel	✗	Dipersyaratkan	Sudah diterapkan jalur dan tracking	✓	Dipersyaratkan	Sudah diterapkan jalur dan tracking	✓
7	**Persyaratan sistem pemadaman kebakaran**												
7.1	Sistem deteksi kebakaran	Dipersyaratkan	Sudah diterapkan sistem sensor deteksi kebakaran.	✓	Dipersyaratkan	Sudah diterapkan sistem sensor deteksi kebakaran.	✓	Dipersyaratkan	Sudah diterapkan sistem sensor deteksi kebakaran.	✓	Dipersyaratkan	Sudah diterapkan sistem sensor deteksi kebakaran.	✓
7.2	Sistem pemadam berbahan gas	Diperbolehkan	Sudah diterapkan sistem pemadam berbahan Gas.	✓	Diperbolehkan	Sudah diterapkan sistem pemadam berbahan Gas.	✓	Diperbolehkan	Sudah diterapkan sistem pemadam berbahan Gas.	✓	Diperbolehkan	Sudah diterapkan sistem pemadam berbahan Gas.	✓
8	**Persyaratan sistem monitoring lingkungan pusat data**												
8.1	Sistem monitoring baterai	Tidak dipersyaratkan	Belum diterapkan sistem monitoring pada baterai	✓	Tidak dipersyaratkan	Belum diterapkan sistem monitoring pada baterai	✓	Dari sistem UPS	Belum diterapkan sistem monitoring pada baterai	✗	Tiap unit baterai, monitoring tahanan dan tegangan	Belum diterapkan sistem monitoring pada baterai	✗

JAIC e-ISSN: 2548-6861

9	Persyaratan keamanan fisik - Ruang peralatan												
9.1	Ruang genset	kunci pengaman standar industri	Sudah diterapkan kunci pengaman setandar	✓	kunci pengaman standar industri	Sudah diterapkan kunci pengaman setandar	✓	kartu akses elektronik	Belum diterapkan	✗	kartu akses elektronik dan biometrik	Belum diterapkan	✗
9.2	Ruang UPS, telepon dan ruang mekanikal elektrikal	kunci pengaman standar industri	Sudah diterapkan kunci pengaman setandar	✓	kunci pengaman standar industri	Sudah diterapkan kunci pengaman setandar	✓	kartu akses elektronik	Belum diterapkan	✗	kartu akses elektronik dan biometrik	Belum diterapkan	✗
9.3	Ruang kontrol pusat data	kunci pengaman standar industri	Sudah diterapkan kunci pengaman setandar	✓	kunci pengaman standar industri	Sudah diterapkan kunci pengaman setandar	✓	kartu akses elektronik	Belum diterapkan	✗	kartu akses elektronik dan biometrik	Belum diterapkan	✗
10	Persyaratan keamanan fisik - Perimeter												
10.1	Membangun pintu masuk dengan pos pemeriksaan keamanan	Tidak dipersyaratkan	Sudah diterapkan pada pintu masuk gedung	✓	Area server	Belum diterapkan	✗	area server, area bongkar muat, dan ruang penyimpanan	Belum diterapkan	✗	area server, area bongkar muat, dan ruang penyimpanan	Belum diterapkan	✗
10.2	Pencatatan tamu atau pengunjung	Manual	Pencatatan tamu dan pengisian dokumen authorisasi	✓	Manual	Pencatatan tamu dan pengisian dokumen authorisasi	✓	manual dan elektronik - digital	Belum diterapkan	✗	manual dan elektronik - digital	Belum diterapkan	✗

Tabel 3.2 *Analisis GAP, Menejemen pusat data*

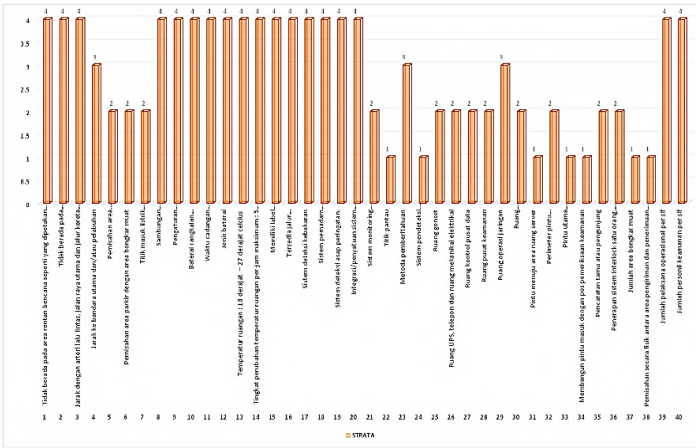
SPESIFIKASI MANAJEMEN PUSAT DATA													
SNI 8799		STRATA 1			STRATA 2			STRATA 3			STRATA 4		
No	Manajemen	Tinjauan Kebutuhan	Kondisi	Cross/ Check	Tinjauan Kebutuhan	Kondisi	Cross/ Check	Tinjauan Kebutuhan	Kondisi	Cross/ Check	Tinjauan Kebutuhan	Kondisi	Cross/ Check
1	Pelaksana Operasional												
1.1	Penyediaan pelaksana operasional	Tidak ada sif dan bekerja dalam jam kerja normal	Sudah diterapkan terbagi dengan 2 sif.	✗	2 orang per sif atau lebih, 24/7/365	Sudah diterapkan terbagi dengan 2 sif.	✗	2 orang per sif, 24 jam - hari kerja	Sudah diterapkan terbagi dengan 2 sif.	✓	2 orang per sif atau lebih 24/7/365	Sudah diterapkan terbagi dengan 2 sif.	✓
2	Infrastruktur Lokasi Pusat data												
2.1	Merefer pada SNI Pusat Data bagian 1, Pemilihan LokasiPenyelenggara pusat data dalam melakukan pembangunan pusat data harus memperhatikan persyaratan lokasi pusat data sebagaimana yang tercantum pada panduan spesifikasi teknis pusat data.	Dipersyaratkan	Sudah diterapkan	✓	Dipersyaratkan	Sudah diterapkan	✓	Dipersyaratkan	Sudah diterapkan	✓	Dipersyaratkan	Sudah diterapkan	✓
3	Manajemen fasilitas pusat data												
3.1	Menyusun dan memperbaharui daftar perangkat dan fasilitas pusat data yang berisi, antara lain: 1, Nama; 2, Jenis; 3,Lokasi; 4,fungsi; 5,kepemilikan; 6,siklus daur hidup.	Dipersyaratkan	Sudah diterapkan	✓	Dipersyaratkan	Sudah diterapkan	✓	Dipersyaratkan	Sudah diterapkan	✓	Dipersyaratkan	Sudah diterapkan	✓

Dapat dilihat pada table diatas, bahwa masih terdapat poin-poin yang masih belum memenuhi syarat standarisasi terutama pada standar SNI 8799:2019 Strata 1, Strata 2, Starta 3, Strata 4, sehingga perlu dilakukan perancangan untuk pengembangan keamanan fisik agar ruang *Next Generation Network* dapat terhindar dari resiko ancaman.

Sesuai denga *tabel 3.1* yang mengarahkan pada kondisi saat ini terkait dengan spesifikasi teknis pusat data pada ruang *Next generation network* yang sebenarnya, spesifikasi teknis pusat data dalam analisa gap terdapat 10 Sub aspek dalam audit diantaranya :

1) Spesifikasi Teknis pemilihan gedung
2) Spesifikasi Area Parkir kendaraan
3) Spesifikasi persyaratan catu daya listrik pusat data
4) Spesifikasi persyaratan UPS
5) Spesifikasi sistem pendingin
6) Spesifikasi persyaratan sistem jaringan pusat data
7) Spesifikasi persyaratan sistem pemadam kebakaran
8) Spesifikasi sistem monitor lingkungan pusat data
9) Spesifikasi persyaratan keamanan fisik
10) Spesifikasi keamanan fisik.

Analisis GAP pada *tabel 3.1* memvisualisasikan perbandingan antara tingkat strata dalam kondisi saat ini pada PT.Telkom Indonesia. Gambar grafik berikut memberikan gambaran yang jelas tentang seberapa jauh ruang prangkat *Next generation network* dari tingkat spesifikasi teknis keamanan secara fisik.

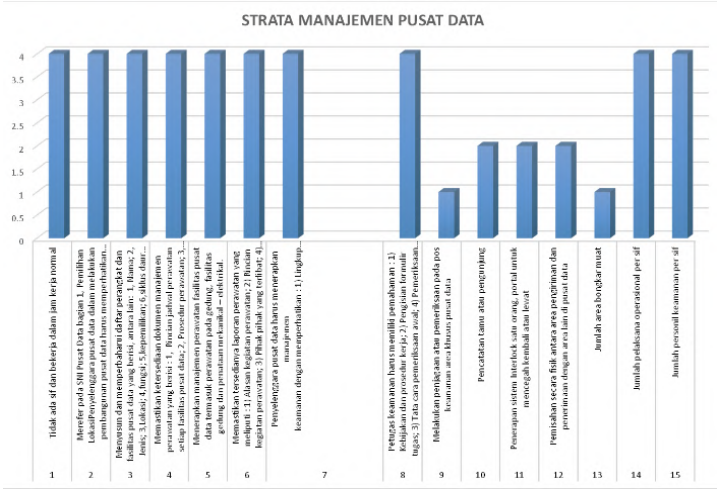


Gambar 3.1,Hasil analisis Gap, Spesifikasi teknis pusat data

Pada *tabel 3.2* terdapat tabel yang mengarahkan kondisi saat terkait dengan spesifikasi menejemen pusat data pada PT.Telkom Indonesia, spesifikasi menejemen pusat data dalam analisis gap terdapat 5 Sub aspek dalam audit diantaranya :

1) Spesifikasi pelaksana operasional
2) Spesifikasi infrastruktur lokasi pusat data
3) Spesifikasi manajemen pusat data
4) Spesifikasi manajemen keamanan pusat data
5) Spesifikasi persyaratan manajemen keamanan pusat data.

Analisis GAP pada *tabel 3.2* memvisualisasikan perbandingan antara tingkat strata dalam kondisi saat ini pada PT.Telkom Indonesia. Gambar grafik berikut memberikan gambaran yang jelas tentang seberapa jauh ruang perangkat *Next generation network* dari tingkat spesifikasi menejemen keamanan pusat data.



Gambar 3.2, Hasil analisis Gap, Spesifikasi menejemen pusat data

D. Rekomendasi

1) Rekomendasi Perangkat Kontrol Akses

Perangkat Kontrol akses diperlukan untuk membatasi pengguna untuk mengakses suatu ruang dengan menempatkan sistem perangkat control pada pintu, jadi hanya staff atau orang-orang yang mempunyai izin akses yang dapat keluar ataupun masuk ke area ruang perangkat *Next Generation Network (NGN).* Berikut merupakan usulan perangkat akses kontrol yaitu berupa perangkat detection dan perangkat card access untuk kebutuhan Strata 3 dan 4 pada standar SNI 8799:2019.

Gambar 3.3 *Visualisasi perangkat Akases Kontrol pada pintu Ruang 1, PT.Telkom Indonesia*

Dapat dilihat pada gambar 3.3 , terdapat penempatan perangkat *Access Door Lock* pada pintu 1 yang berada di tembok atau dinding sebelah pintu, untuk penempatan *Exit Button* di tembok atau dinding sebelah pintu bagian dalam.

Gambar 3.4 *Visualisasi perangkat Akases Kontrol pada pintu Ruang 2, PT.Telkom Indonesia*

Dapat dilihat pada gambar 3.4, terdapat pergantian device pada perangkat *Access Door Lock* pada pintu 2 yang berada di dinding sebelah pintu. Penggunaan *Biometric Control* atau *access door lock* pada kunci, kunci menuju ruang *Next Generation Network* terdapat 2 pintu, dimana pintu pertama masuk ke ruang *NGN* belum menggunakan teknologi *access door lock fingerprint* atau *biometric control*. Dan untuk pintu ke 2 menuju ruang *NGN* sudah menggunakan Kunci *Finger code* namun sudah tidak berfungsi sebagaimana semestinya. Pintu pertama masih menggunakan kunci Konvensional, Kunci konvensional mengandung beberapa resiko seperti kemungkinan untuk hilang dan mudah digandakan. Dengan menggunakan teknologi *biometric control* akses masuk ke Ruang *NGN* akan benar benar terkontrol.

2) Rekomendasi Regulasi Standarisasi

Regulasi standarisasi adalah serangkaian aturan atau pedoman yang dibuat oleh badan pemerintah atau organisasi standar yang bertujuan untuk mengatur dan mengarahkan proses standarisasi. Standarisasi sendiri merujuk pada proses pengembangan, penerapan, dan pemeliharaan standar untuk memastikan keseragaman, kualitas, dan interoperabilitas dalam berbagai bidang seperti teknologi, industry dan lingkungan. Standarisasi yang direkomendasikan ialah SNI 8799 yang mana Standar Teknologi Informasi Pusat Data tersebut tentang Panduan Spesifikasi Teknis Pusat Data yang diadopsi dari standar internasional dari ISO, Uptime dan TIA-942 yang disesuaikan dengan kondisi di Indonesia. SNI 8799-1 dikeluarkan oleh Badan Standarisasi Nasional (BSN). Standar ini menjadi salah satu syarat yang harus dipenuhi oleh berbagai kelembagaan yang menginginkan pusat data yang terstandarisasi nasional.

3) Rekomendasi CCTV

Penambahan *CCTV*, pada area ruang *NGN* pada PT.Telkom indonesia tidak memiliki *CCTV* yang terdedikasi khusus, *CCTV* hanya berada di dalam Ruang *NGN* yang berjumlah 7 Camera *CCTV*, hal ini membuat tidak semua wilayah di sekitar ruang *Next Generation Netwok* ter-cover oleh camera *CCTV*, untuk itu disarankan untuk menambahankan *CCTV* yang khusus yang mengarah ke pintu pertama masuk ke ruang *NGN*. Perlunya penambahan kamera *CCTV* untuk meningkatkan keamanan dan memantau lokasi area gedung serta ruangan yang mengarah ke ruang perangkat *Next Generation Network*.

4) Rekomendasi Kebijakan Area Makan/Minum

Penerapan sistem keamanan fisik pada Ruang *Next Generation Network* juga harus memperhatikan beberapa hal seperti implementasi kebijakan makan, minum, dan merokok, terdapat kebijakan untuk tidak makan, minum dan merokok di lingkungan Ruang *Next Generation Network*, namun wawancara yang dilakukan peneliti mengungkap bahwa pernah pegawai membawa makanan dan minuman masuk ke area *Next Generation Network* ketika ada pekerjaan lembur, dimana hal ini cukup berbahaya bagi ruang *Next Generation Network*. Untuk itu implementasi kebijakan dilingkungan PT.Telkom Indonesia harus di perbaiki, terutama di area Ruang *Next Generation Network* atau pusat data lainnya.

5) Rekomendasi Kebijakan *Vendor*/Tamu

Penerapan sistem menejemen pada Ruang *Next Generation Network* juga harus memperhatikan beberapa hal seperti implementasi kebijakan untuk *Vendor* dalam berkunjung ke ruang *Next Generation Network*, pegawai harus tetap melakukan pengawasan jika ada *vendor* yang masuk ke ruang *NGN* untuk keperluan pekerjaan atau yang lainnya. Dimana hal ini cukup berbahaya bagi ruang *NGN* jika terjadi kelalaian dalam pengawasan pada *vendor*.

6) Rekomendasi UPS (*Uninterruptible Power Supply)*

UPS pada setiap data center atau pusat data telekomunikasi sangant penting, dikarenakan UPS tersebut akan digunakan sebagai cadangangan daya batre sementara jika terjadinya pemadama listrik seketia, dan diperlukan kembali untuk di tingatkan kembali kunci akses pintu pada ruang UPS.

7) Rekomendasi Pelatihan

Kurangnya pelatihan terhadap keamanan fisik pada setiap pegawai yang menyebabkan pegawai PT.Telkom indonesia terlihat kurang mendalami terkait dengan keamanan fisik yang seharusnya diterapkan di pusat data telekomunikasi, maka dari itu perlunya ditingkatkan kembali terkait dengan pelatihan terhadap pegawai terkait dengan keamanan informasi, bukan hanya secara software, melainkan juga secara hardware.

IV. KESIMPULAN

Kesimpulan dari penelitian ini merujuk pada perbaikan dan peningkatan sistem keamanan fisik pada ruang perangkat *Next Generation Network* di PT. Telkom Indonesia sangat penting untuk mengoptimalkan perlindungan terhadap perangkat *NGN* dari potensi ancaman fisik. Berdasarkan analisis tingkat keamanan, observasi kondisi saat ini, dan rekomendasi sesuai dengan panduan SNI 8799:2019, disarankan untuk memperbarui penggunaan kunci konvensional dengan teknologi biometrik, menambah jumlah *CCTV*, menerapkan regulasi standar yang ketat, serta melakukan audit dan pemantauan berkala. Dengan langkah-langkah ini, diharapkan PT. Telkom Indonesia dapat meningkatkan keamanan fisik pada ruang perangkat *NGN* dan menjaga operasional serta keandalan layanan dengan lebih baik.

V. DAFTAR PUSTAKA

[1] Pelco, (2023), Panduan Untuk Kontrol Keamanan Fisik, Perencanaan, Kebijakan Dan Tindakan.

[2] ITU-T/ International Telecommunication Union of Telecommunication, Definisi NGN , ITU:T, Y.2001.

[3] “Data Center Specification Based SNI 8799-1 - Eduparx Blog,” March 30, 2023. https://eduparx.id/blog/training/data-center-specification-based-sni-8799-1/.

[4] Badan Standarisasi Nasional (BSN), (2023), Teknologi Informasi pusat data. Jakarta.

[5] Nuzuli, Salman, And Avon Budiyono, (2020), Analisis Dan Perancangan Keamanan Fisik Data Center Berdasarkan Standar Tia-942 Menggunakan Ppdioo Life-cycle Approach Di Pemerintahan Kabupaten Bandung Barat.

[6] Faza Ainun Nafisah, “Evaluasi Keamanan Informasi Data Center Berdasarkan Standar ISO 27001:2013 (Studi Kasus PT. Pupuk Kalimantan Timur),” n.d.

[7] Musthofa Kamal, Rohmad Saedudin, And Ahmad Almaarif, (2019), “Perancangan Sistem Keamanan Fisik Pada Data Center Cv Media Smart Menggunakan Metode Ndlc Dengan Berdasarkan Standar Tia-942,” N.d.

[8] Digky Bima Priatmoko and Endang Siti Astuti, “(Studi Kasus Pada Unit Penerimaan Mahasiswa Baru Dan Sistem Informasi (PMBSI),” n.d

[9] “Ph_skema_sertifikasi_pusat_data.Pdf.” Accessed June 23, 2024. https://www.bsn.go.id/uploads/download/ph_skema_sertifikasi_pusat_data.pdf.

[10] Miles, Mattew B. dan A. Michael Huberman. 1992. Qualitative Data Analysis: A Sourcebook of New Method. Terjemahan Tjetjep Rohendi Rohidi. Analisis Data Kualitatif: Buku Sumber tentang Metode-metode Baru. Jakarta: Penerbit Universitas Indonesia (UI-PRESS).

[11] Rijali, Ahmad. “ANALISIS DATA KUALITATIF.” Alhadharah: Jurnal Ilmu Dakwah 17, no. 33 (January 2, 2019): 81. https://doi.org/10.18592/alhadharah.v17i33.2374.