Journal of Information Technology and Computer Science (INTECOMS)
Volume 9 Nomor 1, Tahun 2026
e-ISSN : 2614-1574
p-ISSN : 2621-3249

STUDI IMPLIMENTASI SNI ISO/IEC 27001:2022 UNTUK MANAJEMEN RISIKO DATA CENTER BBMKG WILAYAH II

IMPLEMENTASTION STUDY OF SNI/IEC 27001:2022 FOR DATA CENTER RISK MANAGEMENT BBMKG REGION II

Nunuk Irawati[1], Agung Budi Susanto[2], Abu Khalid Rivai[3]
Universitas Pamulang, Tangerang Selatan, Banten[1,2,3]
nunuk.irawati@bmkg.go.id[1]

ABSTRACT

In accordance with Government Regulation No. 95 of 2018 (SPBE) and BMKG Regulation No. 4 of 2020, information is a crucial asset for BBMKG Region II. As an institution responsible for meteorological, climatological, and geophysical data (such as earthquake and tsunami information), data accuracy and security are vital for public safety. Various threats occur, such as web defacement, frequent electrical disturbances that damage servers, thus hampering services that must be real-time, and a lack of information security awareness among employees. This study aims to analyze the readiness and reliability of assets and documents of the BBMKG Region II Data Center, identify threats to information security risks that must be mitigated and controlled, and implement the SNI ISO/IEC 27001:2022 framework in information security risk management. The method used is data collection through interviews, observations, document studies, and Focus Group Discussions (FGD). This study resulted in 30 risks that must be mitigated with a control system from SNI ISO/IEC 27001:2022 which includes 3 (three) risk categories, namely security, infrastructure, and human resources (HR), where one of the indications is the absence of an ISMS policy and an information security operational policy that violates Clause 5.2 - Policy. After handling risks for 3 months including the creation of ISMS documents and information security operational documents, the test results showed a number of 0 major NCs, 4 minor NCs, and 9 OFIs, which illustrates very good for the ISMS status in the BBMKG Region II Data Center

Keywords: *SNI ISO/IEC 27001:2022, Data Center, Risk Management, Information Security Management System (ISMS*)

ABSTRAK

Sesuai dengan PP No.95 Tahun 2018 (SPBE) dan Peraturan BMKG No.4 Tahun 2020, informasi merupakan aset krusial bagi BBMKG Wilayah II. Sebagai institusi yang bertanggung jawab atas data meteorologi, klimatologi, dan geofisika, (seperti info gempa dan tsunami) akurasi dan keamanan data sangat vital bagi keselamatan publik. Berbagai ancaman yang terjadi seperti terjadinya *web defacement*, sering terjadinya gangguan kelistrikan yang merusak server sehingga dapat menghambat layanan yang harus *real time* dan kurangnya kesadaran keamanan informasi dikalangan pegawai. Penelitian ini bertujuan untuk menganalisis kesiapan dan keandalan aset serta dokumen Data Center BBMKG Wilayah II, mengidentifikasi ancaman risiko keamanan informasi keberlangsungan yang harus dimitigasi dan dikontrol, serta melakukan implementasi kerangka kerja SNI ISO/IEC 27001:2022 dalam manajemen risiko keamanan informasi. Metode yang digunakan dengan pengumpulan data melalui wawancara, observasi, studi dokumen, dan Focus Group Discusion (FGD). Penelitian ini menghasilkan 30 risiko yang harus dimitigasi dengan sistem pengendalian dari SNI ISO/IEC 27001:2022 yang meliputi 3 (tiga) kategori risiko, yaitu keamanan, infrastruktur, dan sumberdaya manusia (SDM), dimana salah satu terindikasi adalah belum adanya kebijakan SMKI dan kebijakan operasional keamanan informasi yang melanggar Klausul 5.2 - Kebijakan. Setelah dilakukan penanganan risiko selama 3 bulan diantaranya dengan pembuatan dokumen SMKI dan dokumen operasional keamanan informasi, hasil pengujian menunjukkan sejumlah 0 NC mayor, 4 NC minor, dan 9 OFI, yang menggambarkan sangat baik untuk status SMKI di Data center BBMKG Wilayah II

Kata kunci: SNI ISO/IEC 27001:2022, Data Center, Manajemen Risiko, Manajemen Sistem Keamanan Informasi (SMKI)

PENDAHULUAN

Implementasi manajemen risiko berdasarkan SNI ISO/IEC 27001:2022 pada Data Center BBMKG Wilayah II merupakan kebutuhan mendesak guna menjamin keamanan informasi MKG yang kritis bagi keselamatan publik, sesuai amanat PP No.95 Tahun 2018 tentang SPBE (Pemerintah Pusat, 2018) dan Peraturan BMKG No.4 Tahun 2020

(BMKG, 2020). Studi kasus ini didorong oleh adanya ancaman nyata berupa insiden *web defacement*, gangguan infrastruktur kelistrikan, serta risiko kelalaian manusia, sehingga dilakukan mitigasi sistematis mulai dari identifikasi hingga evaluasi risiko untuk menjaga integritas, kerahasiaan, dan ketersediaan layanan data. Melalui pendekatan praktis, penelitian ini memberikan kontribusi dalam meningkatkan efisiensi kontrol keamanan serta kesiapan dalam menghadapi tantangan digital di lingkungan lembaga pemerintahan.

Data Center BBMKG Wilayah II berfungsi sebagai pusat operasional untuk seluruh sistem aplikasi dan pusat sistem jaringan komunikasi data (Syihabuddin, 2017). Pentingnya ruang ini yang harus menjadi perhatian utama bagi BBMKG Wilayah II yang mengandalkan teknologi informasi untuk menjalankan tugas dan fungsinya. Untuk itu harus dilakukan Sistem Manajemen Keamanan Informasi (SMKI) berbasis SNI ISO/IEC 27001:2022 (BSN, 2023).

Tinjauan Pustaka

Manajemen Risiko

Manajemen risiko merupakan salah satu bagian dari standar SNI ISO/IEC 27001:2022, yang bertujuan untuk menemukan, mengevaluasi, dan menangani ancaman yang terkait dengan sistem manajemen keamanan informasi (SMKI). Tujuan utamanya adalah membantu membuat pilihan yang tepat mengenai ancaman terhadap keamanan menggunakan strategi manajemen risiko yang konsisten dan berulang. Proses manajemen risiko merupakan rangkaian sistematis dari kebijakan, prosedur, dan praktik terhadap aktivitas, penetapan konteks, penilaian risiko (identifikasi risiko, analisis risiko, evaluasi risiko), penanganan risiko, pemantauan dan reviu, serta pencatatan dan pelaporan (MenPANRB RI, 2020).

Risiko atau “risk” merupakan dampak ketidakpastian pada tujuan. Semua kegiatan mengandung risiko yang harus diidentifikasi, dianaliasis, dan dievaluasi. Tujuannanya adalah untuk mengidentifikasi dan mengatasi risiko. Seluruh pemangku kepentingan (*stakeholder)* adalah yang bertanggung jawab untuk memantau, mengevaluasi, dan mengontrol risiko untuk memastikan bahwa tidak ada risiko tambahan. Untuk mencapai tujuan ini, diperlukan komunikasi dan konsultasi dengan seluruh pemangku kepentingan tersebut (Yunarto, 2022).

Risiko dalam hal ini risiko keamanan informasi, merupakan potensi output yang tidak diharapkan dari pelanggaran keamanan informasi oleh ancaman kemanan informasi. Ancaman bisa berupa ancaman internal dan bisa berupa ancaman eksternal. Ancaman internal datang dari personil organisasi atau perusahaan itu sendiri, proses, *force mejeure*, dan infrastruktur, sedangkan ancaman eksternal datang dari *hacker*, tamu, vendor, virus, dan juga bisa berupa bencana alam (Gemilang, 2024).

Sistem Manajemen Keamanan Informasi (SMKI)

Sistem merupakan elemen-elemen yang saling berhubungan. Manajemen merupakan perencanaan, pengorganisasian, pemantauan, pengarahan, dan proses lainnya dalam organisasi. Sehingga, aktivitas melindungi organisasi atau perusahaan dan aset informasinya disebut sebagai sistem manajemen keamanan informasi(Indrajit, Prof., 2011). Sistem manajemen keamanan informasi (SMKI) sangat penting diterapkan agar organisasi atau perusahaan dapat mengelola informasi yang beredar dengan benar dan membuat keputusan berdasartkan informasi tersebut untuk memberikan layanan terbaik kepada pelanggannya. Terdapat empat tahapan dalam SMKI, yaitu identifikasi threats (ancaman), mendefinisikan risiko dari ancaman, menetapkan kebijakan kemanan informasi, dan menerapkan control yang

tertuju pada risiko(Puriwigati & Buana, 2020).

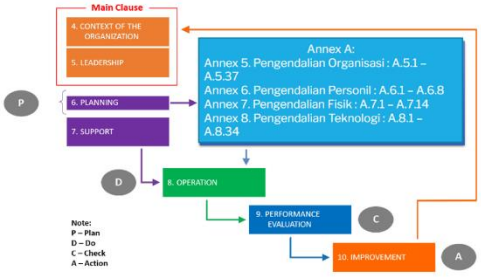
Framework SNI ISO/IEC 27001:2022

Standar Nasional Indonesia (SNI) ISO/IEC 27001:2022 yang berjudul Kemanan informasi, keamanan siber, dan proteksi privasi – Sistem manajemen keamanan informasi – Persyaratan (*Information security, cybersecurity and privacy protection – Information security management systems – Requirements*) merupakan adopsi identik dari Standar Internasional ISO/IEC 27001:2022. Standar ini adalah edisi ketiga dari ISO/IEC 27001 yang merupakan revisi dari SNI ISO/IEC 27001:2013(BSN, 2023).

ISO/IEC 27001:2022 adalah salah satu standar internasional yang paling diakui dalam bidang keamanan informasi, yang memberikan kerangka kerja yang komprehensif bagi organisasi untuk mengidentifikasi, mengelola, dan mengurangi risiko keamanan informasi (IT proxsisgroup, 2024). Dengan menggunakan ISO/IEC 27001:2022, organisasi dapat memastikan bahwa sistem informasi mereka akan terlindungi secara efektif dari berbagai ancaman seperti peretasan, pencurian data, atau gangguan layanan.

a. *Kontrol Klausul dan Annex*

Standar ISO/IEC 27001:2022 memuat 10 klausul. Persyaratan sistem manajemen keamanan informasi dimulai klausul 4 sampai dengan klausul 10, seperti terlihat pada gambar 1 (Gemilang, 2024).



Gambar 1. Klausul dan Annex SNI ISO/IEC 27001:2022

b. *Konsep Plan-Do-Check-Act (PDCA)*

Konsep *Plan-Do-Check- Act* (PDCA) merupakan kerangka kerja fundamental dan siklus dari Sistem Manajemen Keamanan Informasi (SMKI) SNI ISO/IEC 27001:2022. Siklus ini terdiri dari 4 tahap yang berulang yang digunakan untuk implementasi perubahan dan meningkatkan SMKI itu sendiri. PDCA merupakan jantung dari SNI ISO/IEC 27001:2022 karena memastikan bahwa keamanan informasi adalah proses yang terus-menerus (berkelanjutan) dan bukan pekerjaan yang sekali selesai. Setiap siklus PDCA yang telah diselesaikan, akan menghasilkan SMKI yang lebih matang, kuat, dan responsive terhadap ancaman baru (Rizki Septiyanto Wibowo, Tukiyat, Sajarwo Anggai, 2024).

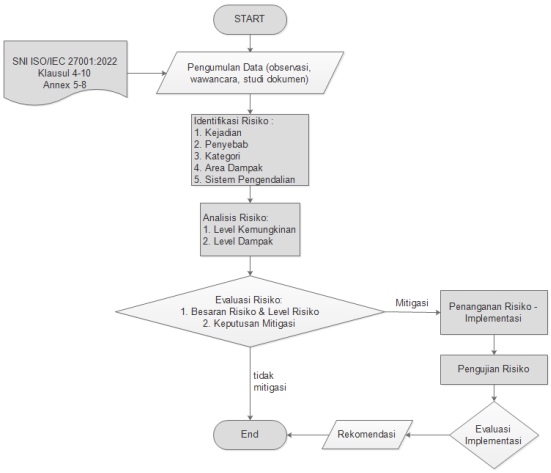
Data Center BBMKG Wilayah II

Data Center adalah ruang yang digunakan untuk mengelola, membackup, dan menyimpan informasi serta server komputer suatu organisasi atau perusahaan yang biasanya terhubung dengan jaringan internet, yang melibatkan banyak elemen dari router, saklar, switch, server, perangkat keamanan, dan elemen pendukung lainnya, yang elemen-elemen tersebut saling berkaitan membentuk jaringan penghimpun informasi(Line, 2018).

Data Center BBMKG Wilayah II berfungsi sebagai pusat operasional serta penyimpanan data dan informasi dalam infrastruktur IT yang di dalamnya terdapat server, switch, dan perangkat jaringan komunikasi lainnya. Ruang ini harus menjaga kinerja perangkat keras, mencegah downtime, dan memastikan keamanan data. Pentingnya ruang ini yang harus menjadi perhatian utama bagi BBMKG Wilayah II yang mengandalkan teknologi informasi untuk menjalankan tugas dan fungsinya.

METODE

Penelitian ini termasuk penelitian deskriptif kualitatif karena menggambarkan kondisi aktual (observasi), wawancara, dan studi dokumen *Data Center* BBMKG Wilayah II(Arsyam & M. Yusuf Tahir, 2021).



Gambar 2. *Flowchart* Langkah Peneltitian

Langkah-Langkah Penelitian

Berdasarkan gambar 1. *flowchart* langkah-langkah penelitian diatas penjelasannya sebagai berikut. Analisis kebutuhan dalam penelitian ini adalah proses sistematis untuk mengidentifikasi dan mendokumentasikan kesenjangan antara kondisi manajemen risiko Data Center di BBMKG Wilayah II dengan persyaratan pada SNI ISO/IEC 27001:2022. Analisis kebutuhan dalam penelitian ini meliputi:

a. Wawancara dilakukan untuk menggali informasi dari personil yang terkait dengan Data Center BBMKG Wilayah II yaitu Kepala BBMKG Wilayah II sebagai top management, Ketua TIM kerja Jaringan Komunikasi, Admin LAN dan Internet, Admin ruang server, dan Petugas dinas shift. Wawancara ini dilakukan untuk mendalami sejauh mana manajemen risiko dilakukan di lapangan, apa saja tantangannya dan apa yang menjadi kebutuhan.
b. Studi dokumentasi ini akan dilakukan pengumpulan data berupa dokumen-dokumen yang relevan seperti kebijakan dan prosedur, pemeriksaan kontrol keamanan teknologi, dan dokumen terkait kompetensi.
c. Observasi dilakukan dengan pengamatan secara langsung kondisi fisik Data Center guna memvalidasi informasi yang diperoleh dari studi dokumen maupun wawancara.

Langkah selanjutnya adalah Pengolahan data yang dimulai dengan identifikasi risiko (*risk identification*). Setelah dilakukan identifikasi risiko, langkah penting berikutnya adalah analisis risiko untuk menentukan tingkat keparahan dan kemungkinan terjadinya risiko tersebut. Tahap penting berikutnya adalah evaluasi risiko. Langkah ini dilakukan untuk menentukan mana penanganan risiko yang paling tinggi dan langkah apa yang harus diambil untuk mengelola risiko.

Penanganan Risiko dilakukan sebagai implementasi kontrol SNI ISO/IEC 27001:2022 terhadap hasil penilaian risiko. Hasil evaluasi risiko dinyatakan risiko diterima dan risiko tidak diterima (mitigasi). Fase ini adalah proses mengubah rencana menjadi tindakan nyata, kontrol keamanan yang sesuai (berdasarkan SNI ISO/IEC 27001:2022), diimplementasikan dalam sistem dan proses operasional. Setelah menerapkan kontrol, risiko dievaluasi kembali dengan tujuan untuk mengukur efektivitas, yaitu menilai apakah kontrol yang diterapkan berfungsi sesuai dengan harapan yaitu menurunkan risiko.

Teknik Analisis

Teknik analisis data dalam hal ini teknik analisis kualitatif adalah serangkaian metode yang digunakan dalam menganalisis data, memahami bagaimana proses dijalankan, untuk mengetahui risiko keamanan informasi pada data yang sudah dikumpulkan. Teknik analisis kuantitatif digunakan untuk menganalisis data insiden, tingkat kepatuhan, juga besaran dan level risiko. Untuk menentukan besaran risiko, matriks risiko akan menggabungkan level kemungkinan dan level dampak. Hasil dari

matriks risiko ditunjukkan dalam bentuk angka.

Tabel 1. Matriks Risiko

		Dampak				
		1	2	3	4	5
Kemungkinan		Tidak Signifikan	Kurang Signifikan	Cukup Signifikan	Signifikan	Sangat Signifikan
5	Hampir Pasti Terjadi	9	15	18	23	25
4	Sering Terjadi	6	12	16	19	24
3	Kadang-Kadang Terjadi	4	10	14	17	22
2	Jarang Terjadi	2	7	11	13	21
1	Hampir Tidak Terjadi	1	3	5	8	20

Tabel 2. Level Risiko

Level Risiko		Rentang Besaran Risiko	Keterangan Warna	Keputusan
1	Sangat rendah	1 – 5	Biru	Terima
2	Rendah	6 – 10	Hijau	Terima
3	Sedang	11 – 15	Kuning	Mitigasi
4	Tinggi	16 – 20	Jingga	Mitigasi
5	Sangat Tinggi	21 – 25	Merah	Mitigasi

Pengujian risiko dilakukan melalui *Fokus Group Discussion* (FGD)(Nafisatur, 2024), yaitu audit internal sesuai dengan klausul 9 pada SNI ISO/IEC 27001:2022. FGD memungkinkan auditor untuk menguji pemahaman kolektif, prosedur yang tidak tertulis, dan skenario yang melibatkan risiko yang telah dimitigasi. Pengujian risiko juga dilakukan melalui konvensional pada pemeriksaan bukti fisik dan rekaman (*hard evidence*).

HASIL DAN PEMBAHASAN

Analisis Kesenjangan

Analisis kesenjangan (gap analysis) adalah metode yang digunakan untuk membandingkan kondisi aktual suatu instansi atau organisasi, proses, atau sistem dengan kondisi yang diinginkan atau ideal. Tujuannya adalah untuk mengidentifikasi perbedaan antara kondisi saat ini dengan target atau standar yang diharapkan, serta mengembangkan rencana tindakan untuk mengurangi kesenjangan tersebut(Marliana et al., 2024).

Berdasarkan hasil wawancara, peninjauan dokumen serta observasi menunjukkan adanya kesenjangan terhadap 4 dari 23 kontrol klausul, dan 36 dari 92 kontrol Annex A.

Penilaian Risiko

Penilaian risiko merupakan proses identifikasi, analisis, dan evaluasi risiko. Tujuan penilaian risiko ini adalah untuk mengetahui penyebab, kemungkinan, dampak risiko, dan besaran risiko yang akan menentukan keputusan apakah diperlukan penanganan risiko atau tidak.

Hasil identifikasi risiko Data Center BBMKG Wilayah II terdapat 30 risiko yang masuk dalam kategori keamanan, infrastruktur, dan Sumber Daya Manusia (SDM). Pada tingkat kemungkinan, hasil analisi menunjukkan bahwa risiko yang dihadapi Data Center BBMKG Wilayah II memiliki tingkat kemungkinan yang sangat tinggi. Mayoritas berisiko (57%), ditetapkan pada level “Hampir Pasti Terjadi” yakni pada 17 kejadian dengan frekuensi lebih dari 12 kali dalam periode tertentu. Risiko sedang (43%) terbagi pada level “Sering Terjadi” yakni pada 5 kejadian dan “Kadang-kadang Terjadi” yakni pada 6 kejadian. Berdasarkan tingkat dampak, dampak yang ditimbulkan cenderung signifikan, dengan dampak utama yaitu level atau tingkat “Cukup Signifikan” yakni berdasarkan dari 17 kejadian) dan level atau tingkat “Signifikan” yakni pada 9 kejadian, sementara terdapat dampak “Sangat Signifikan” yang tercatat pada 3 kejadian.

Hasil evaluasi risiko dengan konsentrasi risiko pada level Tinggi dan Sangat Tinggi menjunkkan bahwa Sistem Pengendalian yang ada belum dilakukan dalam mengurangi risiko, sehingga diperlukan segera melakukan Sistem Pengendalian tersebut. Seluruh risiko yakni sejumlah 30 risiko memiliki keputusan Mitigasi. Hal ini sesuai dengan tingkat risiko yang ditemukan. Keputusan untuk melakukan mitigasi pada semua risiko menunjukkan bahwa Data Center BBMKG Wilayah II telah menerima hasil evaluasi dan mengakui bahwa risiko tersebut berada di luar selera risiko yang dapat ditoleransi. Akibatnya, rencana perlakukan risiko (mitigasi) yang mendalam dan cepat, sangat diperlukan

untuk menurunkan tingkat risiko ke batas yang dapat diterima.

Penanganan dan Pengujian Risiko

Penanganan risiko dilakukan terhadap 30 keputusan mitigasi dari 6 level risiko sedang, 18 resiko tinggi dan 6 risiko sangat tinggi. Penangan risiko dilakukan dengan 40 sistem pengendalian SNI ISO/IEC 27001:2022, yaitu 4 klausul dan 36 annex.

Tahap berikutnya adalah bersertifikasi independent melalui audit internal sebagai pengujian risiko. Audit internal berperan sebagai mekanisme *Check* dalam siklus PDCA (*Plan-DO-Check-Act*) yakni menguji apakah tindakan penanangan risiko telah dilakukan secara benar dan efektif dalam menurunkan risiko ke tingkat yang dapat diterima (*residual risk*).

Hasil pengujian menujukkan terdapat temuan sejumlah 9 OFI (*Opportunity for Improvement*), 4 NC minor (*Non-Conformity minor*), dan 0 NC mayor, memberikan gambaran yang sangat baik mengenai status SMKI di Data Center BBMKG Wilayah II. Hasil 0 NC mayor menunjukkan tidak adanya kegagalan sistematis atau kelemahan yang fatal yang akan mengancam efektivitas keseluruhan dari SMKI. Hasil ini sangat baik dan memperlihatkan dasar sistem yang sudah kuat. Hasil 4 NC minor (*Non-Conformity minor*) menunjukkan adanya penyimpangan prosedur tunggal atau kegagalan parsial dalam memenuhi persyaratan Klausul ISO atau kontrol Annex A. Ini merupakan masalah yang memerlukan perbaikan segera (*correction*) yang diikuti oleh tindakan korektif. Sedangkan hasil 9 OFI (*Opportunity for Improvement*) menunjukkan bukan ketidaksesuaian, melainkan rekomendasi untuk dilakukan peningkatan efisiensi, efektivitas atau kematangan SMKI di atas persyaratan standar minimum.

Evaluasi Implementasi dan Rekomendasi

Secara umum, pelaksanaan SMKI di Data Center BBMKG Wilayah II sudah berjalan dengan baik. Berdasarkan implementasi kontrol dan prosedur yang talah dilakukan sudah berjalan sesuai dengan kerangka kerja SNI ISO/IEC 27001:2022 dan berhasil lolos dari risiko kegagalan sistematis (*Major NC*). Perbaikan di fokuskan pada kegagalan yang bersifat minor yaitu sejumlah 4 NC minor, karena temuan ini menandakan ada beberapa kontrol mitigasi risiko yang belum dijalankan secara konsisten atau prosedurnya belum sempurna. Tindakan berupa koreksi (*Correction*) yaitu tindakan segera guna menghilangkan temuan ketidaksesuaian, serta tindakan korektif (*Corrective action*) yaitu analisis akar masalah dan implementasi tindakan untuk mencegah terulang kembali ketidaksesuaian di masa yang akan datang.

PENUTUP

KESIMPULAN

Berdasarkan hasil studi implementasi SNI ISO/IEC 27001:2022 untuk manajemen risiko Data Center BBMKG Wilayah II, dapat disimpulkan:

a. Hasil penilaian kesenjangan Data Center BBMKG Wilayah II terdapat 30 indikasi Gap terhadap standar SNI ISO/IEC 27001:2022 yang tergolong dalam 3 (tiga) kategori risiko, yaitu keamanan, infrastruktur, dan sumberdaya manusia (SDM). Salah satu gap kategori risiko keamanan dengan level sangat tinggi yang terindikasi adalah belum adanya kebijakan SMKI dan kebijakan operasional keamanan informasi. Kategori infrastruktur salah satu gap terindikasi yaitu belum adanya CCTV di ruang server dan ruang kerja staf jaringan komunikasi yang termasuk dalam level risiko tinggi. Sedangkan kategori risiko SDM salah satunya adalah kurangnya awareness karena

belum dilakukannya peningkatan kompetensi terhadap personel Data Center yang termasuk risiko level sangat tinggi.

b. Penanganan risiko penelitian ini dilaksanakan selama 3 bulan terhadap 30 terindikasi gap sejumlah 6 level risiko sedang (20%), 18 risiko tinggi (60%), dan 6 risiko sangat tinggi (20%), dengan sistem pengendalian SNI ISO/IEC 27001:2022 pada 4 klausul (klausul 5.2 - Kebijakan, Klausul 7.2 - Kompetensi, Klausul 7.5 - Informasi Terdokumentasi, dan Klausul 9.1 - Pemantauan, Pengukuran, Analisis, dan Evaluasi) serta pada 36 Annex (diantaranya Annex A.6.3 - Kesadaran, Pendidikan, dan Pelatihan Keamanan Informasi serta Annex A.7.5. Perlindungan dari Ancaman Fisik dan Lingkungan). Penanganan risiko diantaranya dengan membuat dokumen SMKI, memberikan training pada personel Data Center, serta pemasangan CCTV di ruang server dan ruang Jaringan Komunikasi.

c. Hasil pengujian risiko masih terdapat temuan sejumlah 9 OFI, 4 NC Minor, dan 0 NC Mayor. Diantaranya belum dilakukan kalibrasi alat ukur suhu dan kelembaban (kesenjangan Annex A.7.13 – pemeliharaan Peralatan) yang termasuk dalam temuan NC Minor, serta beberapa dokumen yang belum lengkap (beberapa aset yang belum ada SN) yang termasuk dalam temuan OFI..

Saran yang diberikan untuk penelitian berikutnya pada pelaksanaan SMKI di Data Center BBMKG Wilayah II kedepannya, disarankan melakukan beberapa langkah sebagai berikut:

a. Masalah waktu penelitian yang terbatas (6 bulan) merupakan hambatan bagi peneliti, saran untuk penelitian selanjutnya adalah waktu penilitian minimal dalam 1 (satu) tahun yaitu satu periode kegiatan organisasi agar hasil penelitian lebih maksimal.

b. Kegiatan SMKI merupakan kegiatan rutin yang perlu dimonitor setiap waktu, dengan standar SNI ISO/IEC yang semakin berkembang seiring perkembangan teknologi, sehingga penelitian yang serupa bisa dilakukan secara terus menerus.

DAFTAR PUSTAKA

Arsyam, M., & M. Yusuf Tahir. (2021). Ragam Jenis Penelitian dan Perspektif. *Al-Ubudiyah: Jurnal Pendidikan Dan Studi Islam*, *2*(1), 37–47. https://doi.org/10.55623/au.v2i1.17

BMKG. (2020). Peraturan Badan Meteorologi, Klimatologi, dan Geofisika Republik Indonesia Nomor 4 Tahun 2020. *Bmkg.Go.Id*, *15*(1), 96.

BSN. (2023). *Sni Iso Iec 27001-2022 (2023)*.

Gemilang, P. N. (2024). *AWARENESS ISO 27001 : 2022 SISTEM MANAJEMEN KEAMANAN INFORMASI*.

Indrajit, Prof., R. E. (2011). *Manajemen keamanan informasi*. *1*, 1–19. https://doi.org/12.01.123

IT proxsisgroup. (2024). *Mengintegrasikan Manajemen Risiko ke dalam ISO 27001:2022*. Artikel. https://it.proxsisgroup.com/mengintegrasikan-manajemen-risiko-ke-dalam-iso-270012022/

Line, C. (2018). □□ □□□□□ *Data Center* □□□□ □ □□□ □□□□□□ *Data Center Center Data* □□□□□□ □□. 1–5.

Marliana, E., Nurhadryani, Y., & Hermadi, I. (2024). Analisis Kesenjangan Pemenuhan Standar Sistem Manajemen Keamanan Informasi pada Ina-Geoportal Compliance Gap Analysis of Information Security Management System Standards on Ina-Geoportal. *Ilmu Komputer Agro-Informatika*, *11*(1), 27–38. http://journal.ipb.ac.id/index.php/jika

MenPANRB RI. (2020). PermenPAN RB Nomor 5 Tahun 2020. *MenPAN RB*,

JDIH, *5*(261), 1689–1699.

Nafisatur, M. (2024). Metode Pengumpulan Data Penelitian. *Metode Pengumpulan Data Penelitian*, *3*(5), 5423–5443.

Pemerintah Pusat. (2018). Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. *Menteri Hukum Dan Hak Asasi Manusia Republik Indonesia*, 110.

Puriwigati, A. N., & Buana, U. M. (2020). Sistem Informasi Manajemen-Keamanan Informasi. *Artikel*, *May*.

Rizki Septiyanto Wibowo, Tukiyat, Sajarwo Anggai, W. (2024). Analisis Dan Implementasi Sistem Manajemen Keamanan Informasi Menggunakan ISO/IEC 27001 (Studi Kasus Pada PT.XYZ). *Jurnal Ilmu Komputer Vol.2 Nomor.2, Desember, 2024*, *07*(12), 85–90.

Syihabuddin, A. (2017). Manajemen Risiko Proyek Pengembangan Data Center Instansi XYZ. *Keamanan Jaringan Informasi, Jurusan Teknik Elektro*, *1*, 1–15.

Yunarto, S. (2022). Analisis Manajemen Risiko Pengadilan Negeri Nanga Bulik. *Pengadilan Negeri Nanga Bulik KElas II*, 1–30. https://pn-nangabulik.go.id/images/dokumen/Dokumen Manajemen Resiko.pdf