ANALISIS STANDAR ISO/IEC 27001: 2013 SEBAGAI STRATEGI KEAMANAN INFORMASI DI PUSAT PERTAHANAN SIBER KEMENTERIAN PERTAHANAN REPUBLIK INDONESIA

ANALYSIS OF ISO / IEC 27001: 2013 AS AN INFORMATION SECURITY STRATEGY IN THE SIBER DEFENSE CENTER, MINISTRY OF DEFENSE REPUBLIC OF INDONESIA.

Azizi Algi[1], Agus H. S. Reksoprodjo[2], Rudy Agus G. Gultom[3]

PROGRAM STUDI PEPERANGAN ASIMETRIS/ FAKULTAS STRATEGI PERTAHANAN/ UNIVERSITAS PERTAHANAN
hprojects26@gmail.com

Abstrak – Seiring dengan majunya teknologi digital dan era keterbukaan informasi, dimana terdapat lebih dari 60.000 serangan siber kepada Kementrian Pertahanan pada tahun 2018. Kementerian pertahanan sebagai instansi yang memiliki informasi kritis terbatas harus dapat menangkal segala upaya akses dan penyalahgunaan informasi kritis. Pushansiber selaku pelaksana tugas pertahanan siber di Kementerian Pertahanan harus siap menghadapi ancaman siber salah satunya adalah ancaman data dan informasi. Penelitian ini mengkaji tingkat keamanan informasi yang ada di Pushansiber dengan menggunakan standar ISO/IEC 27001 sebagai alat ukur. Tujuan studi ini adalah mengidentifikasi penerapan keamanan informasi di Pushansiber, dan menemukan hambatan serta merumuskan strategi keamanan informasi di Pushansiber. Proses pengumpulan data dilakukan dengan obersvasi dan wawancara. Maturity Level dan Kondensasi data digunakan sebagai teknik analisa dalam penelitian ini. Hasil penelitian ini menemukan tingkat keamanan informasi di Pushansiber masih buruk dengan hambatan belum adanya kebijakan setingkat Kementrian yang dapat menjadi acuan dan dasar dalam menerapkan kebijakan internal organisasi terkait keamanan informasi. Dengan munculnya Peraturan Kementerian Pertahanan No.14 Tahun 2019 dapat menjadi acuan bagi Pushansiber mengajukan anggaran di tahun 2020 untuk melakukan studi terkait kebijakan internal organisasi dimana kebijakan keamanan informasi berada didalamnya. Penelitian ini juga mendukung penelitian sebelumnya dimana pengelolaan keamanan informasi harus memperhatikan pihak internal dan eksternal. Khususnya pada organisasi pemerintah yang baru terbentuk, payung hukum menjadi hal yang sangat penting bagi organisasi tersebut.

Kata Kunci: Keamanan Informasi, Pushansiber, ISO 27001:2013, Kebijakan, Peperangan Asimetris

Abstract *– Along with the advancement of digital technology and the era of information disclosure, there were more than 60.000 cyber attacks on the Ministry of Defense in 2018. The Ministry of Defense as an institution that has limited critical information must be able to ward off all efforts to access and misuse critical information. Pushansiber as the implementer of cyber defense tasks in the Ministry of Defense must be prepared to face cyber threats, one of which is the threat of data and information. This study examines the level of information security in Pushansiber by using the ISO / IEC 27001 standard as a measurement tool. The purpose of this study is to identify the application of information security in Pushansiber, and find obstacles and formulate an information security strategy in*

[1] Program Studi Peperangan Asimetris, Fakultas Strategi Pertahanan, Universitas Pertahanan
[2] Program Studi Peperangan Asimetris, Fakultas Strategi Pertahanan, Universitas Pertahanan
[3] Program Studi Teknologi Penginderaan, Fakultas Teknik Pertahanan, Universitas Pertahanan

Pushansiber. The process of data collection is done by observation and interviews. Maturity Level and Condensation data are used as analysis techniques in this study. The results of this study found that the level of information security in Pushansiber is still poor with obstacles that do not yet have a Ministry level-policy that can be a reference and basis for implementing internal organizational policies related to information security. With the emergence of Ministry of Defense Regulation No. 14 of 2019, it can become a reference for Pushansiber to budgeting for nect year to conduct a study related to the internal policies of the organization where information security policies are in it. This study also supports previous research in which information security management must pay attention to internal and external parties. Especially in the newly formed government organizations, the legal umbrella becomes very important for these organizations.

Keywords: *Information Security, Pushansiber, ISO 27001: 2013, Policy, Asymmetric Warfare*

Pendahuluan

Perkembangan dunia digital dan ilmu komputer belum merata di seluruh dunia, negara negara yang lebih maju dapat melakukan eksploitasi kepada negara negara yang belum siap menghadapi serangan di dunia digital. Berkaca pada kejadian tahun 2010 terjadi serangan terhadap instansi pengayaan uranium yang dimiliki oleh Iran. Menurut laporan peneliti Symantec menemukan virus "Stuxnet 0.5" yang berada di mesin yang terinfeksi telah dikembangkan dari tahun 2005 ketika Iran masih menyiapkan fasilitas pengayaan uraniumnya dan virus ditempatkan di fasilitas Natanz pada tahun 2007[4]. Virus ini menyebar melalui perangkat memori USB yang terinfeksi dan memanfaatkan kerentanan dalam sistem operasi Windows Microsoft Corp dan kurangnya pengamanan terhadap akses dan informasi di fasilitas tersebut[5]. Kaspersky Lab menemukan bahwa berdasarkan letak geografis, Iran, India dan Indonesia menjadi yang teratas dalam penyebaran virus ini dimana terdapat 34.138 komputer yang terindikasi telah disusupi oleh Stuxnet[6]. Serangan serangan tersebut sebagian besar menyasar kepada infrastruktur kritis negara, yang merupakan bagian dari strategi peperangan asimetris yaitu dengan usaha yang minimal dapat memberikan dampak yang sangat besar terhadap target atau sasaran.

---

4 Tempo.co, "Virus Stuxnet untuk Melumpuhkan Nuklir Iran", https://dunia.tempo.co/read/464583/virus-stuxnet-untuk-melumpuhkan-nuklir-iran/full&view=ok, 1 Maret 2013, Diakses pada 13 Oktober 2019.

5 Antara News, "Apa itu Stuxnet?", https://www.antaranews.com/berita/222505/apa-itu-stuxnet, 28 September 2010, Diakses pada 13 Oktober 2019.

6 Kompas Tekno, "34.000 Komputer di Indonesia Terinfeksi Stuxnet", Tekno: https://tekno.kompas.com/read/2010/10/04/23074744/34.000.komputer.di.indonesia.terinfeksi.stuxnet, 4 Oktober 2010, Diakses pada 1 Oktober 2019.

Pengamanan terkait Kemanan Informasi sendiri sebenarnya telah diatur oleh berbagai ketentuan termasuk undang-undang dan peraturan kementerian. Berdasarkan Undang – Undang Nomor 11 Peraturan Menteri Komunikasi dan Informatika (PERMEN KOMINFO) Nomor 4 Tahun 2016 menjelaskan bahwa institusi penyelenggara negara yang menerapkan sistem elektronik yang berdampak kepada kepentingan umum, pelayanan publik atau kelancaran penyelenggaraan negara harus menerapkan standar keamanan informasi SNI ISO/IEC 27001[7]. ISO/IEC 27001 merupakan sebuah standar keamanan informasi yang berfokus untuk mengamankan Keamanan informasi terkait kerahasiaan, ketersediaan, dan integritas dari suatu informasi[8].

Dalam Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber, Bab IV bagian Kerangka Kerja Penyelenggaraan Pertahanan Siber, Pada poin ke 4 menjelaskan bahwa dalam melakukan manajemen pengamanan informasi, satker pelaksana bidang data dan informasi di lingkungan Kemhan/TNI harus menetapkan pendekatan asesmen risiko pada organisasi dengan:

1. Mengidentifikasi suatu metodologi asesmen risiko yang sesuai dengan manajemen pengamanan informasi, persyaratan hukum dan perundang-undangan yang berlaku.
2. Mengembangkan kriteria untuk menerima risiko dan mengidentifikasi tingkat risiko yang dapat diterima. Metodologi asesmen risiko yang dipilih harus memastikan bahwa asesmen risiko memberikan hasil yang dapat dibandingkan dan direproduksi[9].

Kerahasiaan, integritas dan ketersediaan dari data-data pendukung kegiatan Kemhan dan TNI merupakan hal yang sangat penting dalam usaha memepertahankan kedaulatan negara Republik Indonesia. Apabila terdapat serangan terhadap data center, baik itu pencurian ataupun perusakan terhadap data strategis Kemhan dan TNI yang dapat dilakukan baik melalui serangan siber seperti yang dialami oleh Kemhan ataupun melalui *social engineering* seperti

[7] Peraturan Kementerian Komunikasi dan Informasi, nomor 4 tahun 2016.

[8] International Standard Organization, "ISO/IEC 27001: 2013", 2013

[9] Peraturan Kementerian Pertahanan, Nomor 82 Tahun 2014, Bab IV

serangan yang terjadi di pengayaan uranium Iran, secara tidak langsung dapat menjadi ancaman bagi kedaulatan bangsa dan negara.

Pushansiber Kemhan selaku pelaksana tata kelola, kerja sama, operasi dan jaminan keamanan pertahanan siber seyogyanya memiliki tanggung jawab dalam menjaga kerahasiaan, integritas dan ketersediaan informasi Kementerian Pertahanan dan TNI. Dalam pengelolaan kemanan informasi menurut Permenhan No.82 tahun 2014, dibutuhkan sebuah analisis resiko dan celah keamanan dalam penerapan manajemen pengamanan informasi[10]. Maka ISO/IEC 27001 yang terbitkan oleh *International Organization for Standarization* (ISO) dan *International Electronical Comission* (IEC) sebagai sebuah standar dan kerangka dalam usaha pengamanan informasi dinilai cocok sebagai alat ukur untuk melihat pengelolaan keamanan informasi yang dilakukan oleh Pushansiber pada data center Kementerian Pertahanan.

Berdasarkan latar belakang tersebut maka penelitian ini akan membahas mengenai "Analisis Standar ISO.IEC 27001:2013 sebagai Strategi Keamanan INformasi di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia".

Berdasarkan latar belakang penelitian diatas, maka terdapat rumusan masalah yang diangkat yaitu Dengan berkembangnya dunia digital beserta berbagai ancamannya dimana keamanan informasi adalah salah satu diantaranya. Kemudian Pushansiber yang memiliki tanggung jawab dalam pengamanan dibidang pertahanan siber di lingkungan Kementerian Pertahanan yang memiliki informasi strategis yang memiliki akses terbatas. Maka dibutuhkan kemampuan Pushansiber dalam menjaga keamanan informasi dari berbagai macam ancaman dimasa damai.

Sejalan dengan Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber, menjelaskan bahwa dalam melakukan manajemen pengamanan informasi, satker pelaksana bidang data dan informasi di lingkungan Kemhan/TNI harus menetapkan pendekatan asesmen risiko pada organisasi. Maka standar Sistem Manajemen Keamanan Informasi, ISO 27001:2013 dapat menjadi salah satu cara untuk melakukan asesmen dan Analisa

[10] Ibid, hal 16

manajemen pengamanan informasi. Berdasarkan permasalah tersebut, maka dirumuskan pertanyaan penelitian sebagai berikut:

1. Bagaimana pengelolaan keamanan informasi di Pushansiber Kemhan yang diukur dengan menggunakan standar keamanan informasi ISO/IEC: 2013?
2. Apakah hambatan dan masalah di dalam pengelolaan keamanan informasi di Pushansiber Kemhan?
3. Bagaimana ISO/IEC 27001: 2013 dapat menjadi Strategi Keamanan Informasi di Pushansiber Kementerian Pertahanan?

Metode Penelitian

Penelitian kualitatif dipergunakan untuk melakukan eksplorasi tehadap fenomena fenomena yang tidak dapat dikuantifikasikan karena bersifat deskriptif seperti proses suatu langkah kerja, formula suatu resep, pengertian pengertian konsep yang beragam, karakteristik barang atau jasa, gambar, gaya, budaya, model dan sebagainya[11]. Penelitian kualitatif merupakan metode penelitian yang berlandaskan pada filsafat *post-positivisme*, peneliti sebagai individu berperan sebagai instrumen kunci, menggunakan triangulasi sebagai Teknik pengumpulan data, analisis bersifat induktif dan kualitatif dan memiliki hasil yang menekankan makna secara kualitatif dibandingkan dengan generalisasi hasil[12].

Patton menjelaskan dalam penelitian kualitatif peneleiti berfokus kepada kata-kata sebagai kutipan dari subjek penelitian untuk memverifikasi dan mengkonfirmasi makna atau maksud dari pesan yang disampaikan pada saat dilakukannya wawancara, yang dilakukan dengan menganalisa setiap kata, dan melaporkan setiap pandangan dari informan penelitian[13]. Kemudian hasil dari analisa tersebut dijabarkan sebagai sebuah narasi yang bertujuan untuk memberikan gambaran dan pemahaman yang menekankan kepada kualitas dalam segi ilmiah, bukan pada perhitungan matematis. Dalam penelitian kualitatif, peneliti menampilkan sebuah gambaran kompleks, meneliti setiap kata, laporan detail dengan sudut pandang responden,

[11] D. Satori & A. Komariah, *Metode Penelitian Kualitatif,* (Bandung: Alfabeta, 2011)

[12] Sugiyono, *Kualitatif dan R&D,* (Bandung: Alfabeta, 2009)

[13] M. Patton, *Qualitative Research & Evaluation Method,* (USA: Sage, 2012)

dan melakukan observasi dan melakukan studi pada situasi yang alami[14].

Pada penelitian ini, data diperoleh dari berbagai sumber dengan berbagai teknik pengumpulan data untuk mendapatkan karakteristik data yang sesuai dengan kebutuhan penelitian ini, salah satunya adalah observasi. Marshall dalam Sugiono mengatakan "*through observation, the researcher learns about behavior and the meaning attached to those behavior*". Melalui observasi, peneliti belajar tentang perilaku dan makna dari perilaku tersebut[15]. Observasi dilakukan untuk mendapatkan data mengenai proses dari implementasi kebijakan keamanan informasi di lingkungan Pushansiber observasi dilakukan menggunakan Standar ISO/IEC 27001:2013 sebagai panduan dan *maturity Level* dari ISACA untuk menggambarkan hasil temuan di lapangan.

Menurut B. Stevanovic dalam Nasser, standar keamanan informasi dapat dinilai dengan memaparkan sebuah model yang dapat dipahami oleh pelaku keamanan informasi dan para ahli. Model kesiapanan atau *Maturity Model* adalah

1. Sekumpulan dari elemen elemen yang terstruktur dan dapat menjabarkan efektifitas dari sebuah proses atau produk.
2. Model ini dapat menjadi acuan dalam menentukan urutan kerentanan elemen keamanan yang harus ditingkatkan, hal ini menjadi acuan standar keamanan dalam menganalisa program keamanan informasi yang diterapkan.
3. Sering digunakan pada ranah keamanan informasi untuk melakukan penilaian terhadap suatu organisasi.
4. Sebagai perangkat perbandingan untuk melakukan evaluasi kemampuan dari organisasi dalam memenuhi keamanan informasi[16].

Maturity model digunakan untuk mendeskripsikan, mengevaluasi, menilai penerapan keamanan informasi dengan meilhat nilai kematangan dan selisih

[14] J. Creswell, *Qualitative Inquiry & Research Design : Choosing Among Five Approaches,* (Thousand Oaks: Sage Publication, 2007)

[15] Sugiyono, OpCit

[16] A. Nasser, "Information security gap analysis based on ISO 27001:2013 standard : A case study of yhe Yemeni Academy for Graduate Studies, Sana's, Yemen", *International Journal of Science research in Multidisciplinary Studies*, 4-13.

diantara level yang dicapai dan level yang diharapkan dengan keterangan sebagai berikut:

1. Perkembangan dari suatu entitas digambarkan dalam skala maksimal tertentu, biasanya dari 4 – 6.
2. Tingkat kematangan dikategorikan dengan mengikuti kebutuhan tertentu yang menjadi acuan dari entitas yang dinilai.
3. Nilai yang diberikan secara berurutan dari tingkat terkecil hingga maksimal, tingkat maksimal dinilai sempurna.

Penelitian ini akan menggunakan skala 0 – 5 yang berdasar kepada *Maturity Model* yang di definisikan sebagai berikut:

Tabel 1. *Maturity Level*

	Kode	Keterangan
0	*Non Existent*	Tidak didapatkan adanya keperluan untuk kontrol internal
1	*Initial / Adhoc*	Terdapat beberapa temuan yang diperlukan kontrol internal
2	*Repeatable But Intutuive*	Kontrol dilakukan namun tidak terdokumentasi
3	*Defined Process*	Kontrol dilakukan dan terdokumentasi
4	*Managed and measurable*	Terdapat kontrol internal yang efektif dan manejemen penganganan resiko
5	*Optimized*	Diterapkan sebuah kontrol dan analisa resiko yang efektif dan berkesinambungan

Sumber : ISACA,2016

Hasil dan Pembahasan

Pengelolaan Keamanan Informasi di Pushansiber Kemhan

Pushansiber selaku pelaksana tata kelola, kerjasama, operasi, dan jaminan keamanan pertahanan siber di lingkungan Kementerian Pertahanan dan juga melakukan pemantauan, evaluasi, pengendalian dan pelaporan di bidang tata kelola, kerja sama, operasi, dan jaminan keamanan pertahanan siber memiliki peran penting dalam pengamanan informasi di lingkungan pertahanan.

Khususnya pada era digital ini, dimana semua sudah terkoneksi secara jaringan dan digital. Sehingga segala informasi dapat dengan mudah dicuri dan dipergunakan untuk kepentingan pribadi dan golongan. Kementerian Pertahanan pada khususnya memiliki informasi strategis mengenai pertahanan yang dimiliki oleh Indonesia. Sehingga data dari Kementerian Pertahanan menjadi sebuah hal vital bagi keamanan dan kedaulatan bangsa dan negara Indonesia. Pushansiber sebagai kekuatan utama yang dimiliki oleh Kementerian Pertahanan dalam upaya mengamankan segala informasi strategis seharusnya

memiliki kemampuan dan budaya yang menunjang tupoksi Pushansiber yaitu Kerahasiaan, Integritas dan Ketersediaan dari Informasi.

Penilaian mengacu kepada poin pembahasan di ISO/IEC 27001 untuk menganalisa celah keamanan informasi yang ada di Pushansiber. Analisa dilakukan dengan melakukan penilaian bersama dengan beberapa staff Pushansiber selaku narasumber. Terdapat 14 poin pembahasan yang didalamnya terdapat 114 poin kontrol yang dinilai dengan menggunakan *maturity level.* Kemudian dilakukan sebuah penilaian secara menyeluruh dengan menjumlah nilai tiap poin kontrol menjadi poin pembahasan yang dicari nilai akhir dengan mencari nilai rata-rata dari nilai poin pembahasan dengan membandingkanya dengan jumlah data. Hasil dari penilaian keamanan informasi di Pushansiber dengan menggunakan standar ISO/IEC 27001 memiliki hasil sebagai berikut:

Tabel 2. Penlitaian *Maturity Level* di Pushansiber

Issue	*Nilai*	*Jumlah Data*	*Nilai Akhir*	*Ranked*
Information security policies	*3*	*2*	*1.5*	*3*
Organization of Information Security	*21*	*7*	*3.0*	*13*
Human resource security	*13*	*6*	*2.2*	*9*
Asset management	*28*	*10*	*2.8*	*12*
Access Control	*35*	*14*	*2.5*	*11*
Cryptography	*4*	*2*	*2.0*	*6*
Physical and environmental security	*30*	*15*	*2.0*	*7*
Operation security	*26*	*14*	*1.9*	*5*
Communication security	*17*	*7*	*2.4*	*10*
System acquisition, development and maintenance	*6*	*13*	*0.5*	*2*
Supplier relationships	*0*	*5*	*0.0*	*1*
Information security incident management	*14*	*7*	*2.0*	*8*
Information security aspects of business continuity management	*9*	*3*	*3.0*	*14*
Compliance	*14*	*8*	*1.8*	*4*

Sumber: Hasil Olahan Peneliti, 2019

Dari hasil observasi yang dilakukan pada tingkat keamanan informasi yang ada di Pushansiber dengan poin kontrol ISO/IEC 27001 sebagai landasan yang

diukur dengan skala dari *maturity level* dapat mendeskripsikan tingkat keamanan informasi secara lebih detail dan akurat. Pada tabel 2, *issue* adalah poin pembahasan yang berlandaskan ISO/IEC 27001, kolom nilai adalah jumlah nilai tiap poin pembahasan yang didapat dari menjumlahkan nilai *maturity level* dari setiap poin kontrol. Jumlah data adalah jumlah poin kontrol yang ada pada setiap poin pembahasan. Nilai akhir merupakan nilai rata-rata *maturity level* tiap poin pembahasan. *Ranked* adalah penilaian prioritas, dimana nilai akhir terendah menjadi prioritas dengan nilai *rangked* 1, begitu seterusnya. Selanjutnya hasil penilaian tiap poin pembahasan dijabarkan untuk mempermudah analisa masalah.

Pada lingkup *information security policies* memiliki sasaran untuk memberikan arahan dan dukungan oleh manajemen untuk keamanan informasi dengan berdasar kepada persyaratan hukum dan relasi yang relevan[17]. Lingkup ini memiliki 2 poin kontrol dengan jumlah nillai *maturity level* tiap poin kontrolnya adalah 3. Untuk mendapatkan nilai akhir pada lingkup ini dilakukan perhitungan yaiu jumlah nilai dibagi jumlah data (poin kontrol), sehingga nilai akhir dari lingkup ini adalah 1,5 artinya belum adanya kontrol secara teknis terkait lingkup ini sehingga diperlukan kontrol. Nilai ini terbilang rendah dibandingkan dengan nilai *maturity level* standar di angka 3. Dari hasil wawancara menjelaskan bahwa rendahnya nilai keamanan informasi pada lingkup kebijakan keamanan informasi dikarenakan belum adanya SOP atau kebijakan internal terkait dengan keamanan informasi di lingkungan Pushansiber. SOP pernah ada waktu Pushansiber masih menjadi *Cyber Operation Center* dan berada di dalam organisasi Pusdatin.

Lingkup pengorganisasian keamanan informasi memiliki dua poin pembahasan yaitu organisasi internal untuk pengelolaan keamanan informasi dalam organisasi dan pemeliharaan keamanan informasi organisasi dan kebijkan terkait alat komunikasi mobile[18]. Lingkup ini memiliki 7 poin kontrol dengan jumlah nillai *maturity level* tiap poin kontrolnya adalah 21. Untuk mendapatkan nilai akhir pada lingkup ini dilakukan perhitungan yaiu jumlah nilai

[17] International Standard Organization, *ISO 27001: 2013*

[18] Ibid

dibagi jumlah data, sehingga nilai akhir dari lingkup ini adalah 3. Nilai ini terbilang cukup dalam memenuhi nilai standar keamanan informasi. Dari hasil wawancara dapat disimpulkan bahwa sudah terdapat tupoksi dalam setiap bagian di Pushansiber yang diukur dengan SKP (Sarana Kinerja Pegawai), selain itu juga terdapat laporan harian, mingguan dan bulanan yang selalu dilaporkan ke Bainstrahan. Kontrol terkait perangkat telekomunikasi *mobile* masih perlu diperhatikan dikarenakan masih memiliki *maturity level* 2. Dari hasil wawancara ditemukan bahwa pada saat masih menjadi COC (*Cyber Operation Center*) Pusdatin, terdapat *jammer* telekomunikasi yang dipasang dan pelarangan menggunakan perangkat telekomunikasi pribadi dilarang di lingkungan Pushansiber, namun pada saat ini tidak dijalankan.

Lingkup keamanan sumber daya manusia memiliki 2 poin pembahasan yaitu pengendalian sebelum penugasan, saat penugasan dan setelah penugasan[19]. Lingkup ini memiliki 6 poin kontrol dengan jumlah nillai *maturity level* tiap poin kontrolnya adalah 13. Untuk mendapatkan nilai akhir pada lingkup ini dilakukan perhitungan yaiu jumlah nilai dibagi jumlah data, sehingga nilai akhir dari lingkup ini adalah 2,2 yang artinya sudah ada kontrol secara teknis pada penanganan berbagai macam issue yang ada di lingkup ini, namun nilai ini terbilang rendah dibandingkan dengan nilai *maturity level* standar di angka 3. Dari hasil wawancara ditemukan bahwa segala hal mengenai pengadaan personel masih diurus dan diatur oleh biro kepegawaian Kementerian pertahanan secara langsung dan Pushansiber tidak memiliki wewenang untuk melakukan *screening* personel.

Manajemen aset membahas mengenai tanggung jawab terhadap asset, pengklasifikasian informasi dan pengaturan media data[20]. Pada lingkup ini memiliki 3 poin pembahasan dengan 10 poin kontrol dan memiliki jumlah nilai *maturity level* sebesar 26. Untuk mendapatkan nilai akhir pada lingkup ini dilakukan perhitungan yaiu jumlah nilai dibagi jumlah data (poin kontrol), sehingga nilai akhir dari lingkup ini adalah 2,8. Nilai ini hampir mencapai *maturity level* 3 yang merupakan standar keamanan informasi pada tahap awal. Dari hasil wawancara ditemukan bahwa

[19] Ibid

[20] Ibid

dalam pelaksanaan sudah ada dokumen untuk serah terima aset dan pengklasidikasian informasi telah diatur secara digital. Untuk keperluan akses terhadap informasi perlu mengajukan permohonan kepada kepala bagian penjamin keamanan. Sedangkan mengenai media penyimpanan yang sudah tidak terpakai belum ada aturan secara tertulis dalam penanganan atau pemusnahan media tidak terpakai tersebut.

Pengendalian akses memiliki empat poin pembahasan yaitu akses control untuk keperluan bisnis, manajamen akses personel, kewajiban personel dan akses kontrol terhadap sistem dan aplikasi[21]. Lingkup ini memiliki 14 poin kontrol dengan jumlah nillai *maturity level* tiap poin kontrolnya adalah 35. Untuk mendapatkan nilai akhir pada lingkup ini dilakukan perhitungan yaiu jumlah nilai dibagi jumlah data (poin kontrol), sehingga nilai akhir dari lingkup ini adalah 2,5. Nilai ini terbilang rendah dibandingkan dengan nilai *maturity level* standar di angka 3.Dari hasil wawancara ditemukan bahwa perihal pengaturan akses keluar masuk gedung dan ruangan telah diatur dan terdokumentasi oleh bagian data center dengan persetujuan Kabidjamkam, tim data center juga memiliki super akun untuk memantau dan mengatur akun lain yang memiliki akses di Pushansiber. Pembatasan akses digital juga sudah dijalankan dengan adanya VPN namun belum terdapat dokumen atau peraturan yang mengatur perihal pembatasan secara fisik dan digital di lingkungan Pushansiber.

Pada lingkup kriptografi ini terdapat satu poin pembahasan yaitu akses control dalam kiptrogafi data[22]. Lingkup ini memiliki 2 poin kontrol dengan jumlah nillai *maturity level* tiap poin kontrolnya adalah 4. Untuk mendapatkan nilai akhir pada lingkup ini dilakukan perhitungan yaiu jumlah nilai dibagi jumlah data (poin kontrol), sehingga nilai akhir dari lingkup ini adalah 2 artinya sudah ada penanganan secara teknis namun belum terdokumentasi dan belum menjadi sebuh kebijakan yang mengatur pelaksanaan teknis harian. Nilai ini terbilang rendah dibandingkan dengan nilai *maturity level* standar di angka 3. Dari hasil wawancara ditemukan bahwa dalam melakukan pengiriman pesan digital dan berbagai macam data dilakukan dengan menggunakan aplikasi internal milik

[21] Ibid

[22] Ibid

Kementerian pertahanan. Namun kebijakan dan perturan yang mewajibkan penggunaan aplikasi tersebut belum ada.

Pengamanan lingkup kerja memiiki dua poin pembahasan yaitu pengamanan area dan peralatan[23]. Lingkup ini memiliki 15 poin kontrol dengan jumlah nillai *maturity level* tiap poin kontrolnya adalah 30. Untuk mendapatkan nilai akhir pada lingkup ini dilakukan perhitungan yaiu jumlah nilai dibagi jumlah data (poin kontrol), sehingga nilai akhir dari lingkup ini adalah 2 artinya sudah ada penanganan secara teknis namun belum terdokumentasi dan belum menjadi sebuh kebijakan yang mengatur pelaksanaan teknis harian. Nilai ini terbilang rendah dibandingkan dengan nilai *maturity level* standar di angka 3. Dari hasil wawancara ditemukan adanya *Face Recognation Device* yang dipasang dapat mencegah orang yang tidak berkepentingan masuk kedalam lingkungan kerja. Analisa resiko di lingkungan kerja belum dibuat dikarenakan belum adanya kebijakan yang mengatur hal tersebut, selanjutnya pengamanan terkait kabel, aset, dan manajemen penanganan peralatan yang dapat menjadi acuan juga belum ada.

Operasi keamanan memiliki tujuh poin pembahasan yaitu prosedur dan tanggung jawab operasional, perlindungan dari *Malware*, *Backup*, pencatatan dan pengawasan, control terhadap penggunaan perangkat lunak, manajemen kelemahan teknis, dan audit terhadap sistem informasi[24]. Lingkup ini memiliki 14 poin kontrol dengan jumlah nillai *maturity level* tiap poin kontrolnya adalah 26. Untuk mendapatkan nilai akhir pada lingkup ini dilakukan perhitungan yaiu jumlah nilai dibagi jumlah data (jumlah poin kontrol), sehingga nilai akhir dari lingkup ini adalah 1,9 dimana pada sebagian poin kontrol sudah ada penanganan secara teknis tapi masih terdapat beberapa poin kontrol yang belum ada penanganan secara teknis, nilai ini terbilang rendah dibandingkan dengan nilai *maturity level* standar di angka 3. Dari hasil wawancara ditemukan belum adanya kontrol yang mengatur apabila ada perubahan dalam pengorganisasian, bisnis proses, fasilitas maupun sistem yang dapat mempengaruhi keamanan informasi di Pushansiber. Kemudian terkait penanganan *malware* sudah dibuat sebuah SOP oleh divisi Data Center dan

[23] Ibid

[24] Ibid

insident handling namun dalam melakukan *backup* untuk keseluruhan sistem dan data Pushansiber belum dapat dilakukan karena keterbatasan sarana dan prasarana. Akibat tidak adanya anggaran untuk mengadakan sarana dan prasarana penunjang, *log* aktifitas digital yang ada di Pushansiber juga tidak dapat di rekam.

Dalam lingkup keamanan informasi terdapat 2 poin pembahasan yaitu manajemen keamanan jaringan dan transfer informasi[25]. Lingkup ini memiliki 7 poin kontrol dengan jumlah nillai *maturity level* tiap poin kontrolnya adalah 17. Untuk mendapatkan nilai akhir pada lingkup ini dilakukan perhitungan yaiu jumlah nilai dibagi jumlah data (jumlah poin kontrol), sehingga nilai akhir dari lingkup ini adalah 2,4 yang artinya sudah beberapa poin kontro yang terdokumentasi namun belum keseluruhan sehingga nilai *maturity level* masih berada dibawah 3. Dijelaskan dalam wawancara bahwa pengelolaan jaringan berupa kontrol dan pembagian jaringan sudah dilakukan secara teknis oleh tim *network* namun belum ada pendifinisian kebijakan yang mendukung untuk tim *network* melakukan pengamanan lebih lanjut dan dalam aktifitas hariannya, karyawan pushansiber bertukar data dan pesan menggunakan aplikasi internal milik Kementerian Pertahanan.

Pengakuisisian, pengembangan dan perawatan sistem memiliki dua poin pembahasan yaitu akses control dalam kiptrogafi data[26]. Lingkup ini memiliki 13 poin kontrol dengan jumlah nillai *maturity level* tiap poin kontrolnya adalah 6. Untuk mendapatkan nilai akhir pada lingkup ini dilakukan perhitungan yaiu jumlah nilai dibagi jumlah data (poin kontrol), sehingga nilai akhir dari lingkup ini adalah 0,5 yang artinya masih banyak poin kontrol yang belum menjadi *concern* bagi pushansiber yang dimana ini masih sangat jauh dari *maturity level* 3 yang merupakan standar awal keamanan informasi. Dari hasil wawancara diteukan bahwa terkait kebutuhan keamanan dalam sistem informasi masih dilakukan secara *by case* artinya apabila ada masalah baru dilakukan penanganan secara teknis. Kemudian pengembangan sistem masih dianggap bukan menjadi bagian dari Pushansiber karena pengembangan seluruh sistem baik itu

[25] Ibid

[26] Ibid

software dan hardware masih dilakukan di Pusdatin.

Pada lingkup yang membahas hubungan dengan supplier atau vendor terdapat dua poin pembahasan yaitu keamanan informasi dalam berhubungan dengan *supplier* dan manajemen penerapan jasa *supplier*[27]. Lingkup ini memiliki 5 poin kontrol dengan jumlah nillai *maturity level* tiap poin kontrolnya adalah 0. Untuk mendapatkan nilai akhir pada lingkup ini dilakukan perhitungan yaiu jumlah nilai dibagi jumlah data (poin kontrol), sehingga nilai akhir dari lingkup ini adalah 0 yang artinya Pushansiber masih menganggap belum adanya kepentingan bagi Pushansiber untuk berkomunkasi dengan *supplier.* Sejalan dengan hasil wawancara yang menemukan belum adanya dasar kebijakan untuk Pushansiber membuat anggaran.

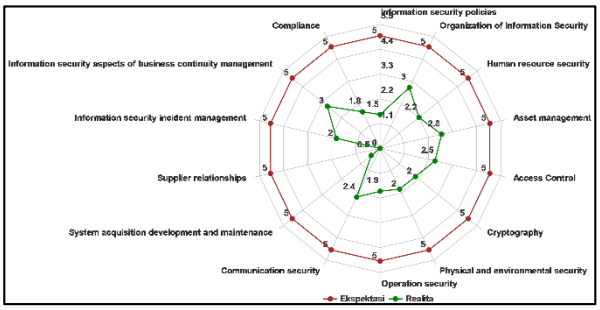
Dalam lingkup penanganan insiden keamanan informasi terdapat satu poin pembahasan yaitu manajemen dalam insiden keamanan informasi dan pengembangannya[28]. Lingkup ini memiliki 7 poin kontrol dengan jumlah nillai *maturity level* tiap poin kontrolnya adalah 14. Untuk mendapatkan nilai akhir pada lingkup ini dilakukan perhitungan yaiu jumlah nilai dibagi jumlah data (poin kontrol), sehingga nilai akhir dari lingkup ini adalah 2 artinya sudah ada penanganan terkait kontrol pengamanan informasi namun hanya di ranah teknis dan belum menjadi sebuh dokumen dan kebijakan. Dari hasil wawancara menemukan sudah dibentuk sebuah tim CERT untuk penanganan insiden namun SOP internal Pushansiber belum ada dikarenakan belum adanya rujukan.

Aspek keberlangsungan keamanan informasi memiliki dua poin pembahsan yaitu kelanjutan keamanan informasi dan ketersediaan fasilitas[29]. Lingkup ini memiliki 3 poin kontrol dengan jumlah nillai *maturity level* tiap poin kontrolnya adalah 9. Untuk mendapatkan nilai akhir pada lingkup ini dilakukan perhitungan yaiu jumlah nilai dibagi jumlah data (poin kontrol), sehingga nilai akhir dari lingkup ini adalah 3 yang artinya sudah ada sebuah kebijakan yang mengatur kontrol. Meurut hasil wawancara bahwa didalam masa krisis ada *Disaster Recovery Center* di Sentul yang dapat menjadi *backup planning* dalam mengamankan data dan sistem kementerian pertahanan.

[27] Ibid
[28] Ibid
[29] Ibid

Lingkup yang terakhir adalah pengaplikasian SMKI yang memiliki dua poin pembahasan yaitu pengaplikasian sesuai dengan legal dan control yang dibutuhkan serta adanya review keamanan infromasi[30]. Lingkup ini memiliki 8 poin kontrol dengan jumlah nillai *maturity level* tiap poin kontrolnya adalah 14. Untuk mendapatkan nilai akhir pada lingkup ini dilakukan perhitungan yaiu jumlah nilai dibagi jumlah data (poin kontrol), sehingga nilai akhir dari lingkup ini adalah 1,8 yang artinya penerapan sistem manajemen keamanan informasi di lingkungan Pushansiber masih jauh dibawah *maturity level* 3. Dari hasil wawancara menemukan bahwa yang perlu diperhatikan adalah aspek legal dalam penerapan SMKI di Pushansiber masih belum terpenuhi dan belum adanya *review* secara berkala oleh internal organisasi terkait keamanan informasi di lingkungan Pushansiber.

Pada tabel 2 kolom bagian *Ranked* adalah nilai yang didapatkan dengan cara mengurutkan dari nilai terkecil pada kolom nilai akhir. *Supplier Relationship* mendapatkan rangking 1 dikarenakan memiliki nilai akhir terkecil yaitu 0. Hal ini menyebabkan *Supplier Relationship* menjadi prioritas utama dalam perbaikan keamanan informasi di Pushansiber. Prioritas perbaikan keamanan informasi di Pushansiber dapat mengikuti kolom *Rangked* dari nilai rangking 1 hingga rangking 14. Untuk memudahkan Analisa, ke 14 poin pembahasan dan nilai rata-rata dari masing masing poin dibuat suatu grafik untuk menampilkan keadaan eksisting dan ekspektasi dari tingkat keamanan informasi yang ideal. Maka data tersebut disajikan dalam grafik dibawah ini:



Gambar 1. Nilai Aktual Keamanan Informasi
Sumber: Hasil Olahan Peneliti, 2019

Menurut standar ISO/IEC 27000: 2018, Keamanan informasi adalah usaha untuk memastikan kerahasiaan, ketersediaan, dan integritas dari suatu informasi[31]. Kemanaan informasi didapatkan dengan melaksanakan kontrol yang terintegrasi dengan manajemen resiko yang diatur didalam

[30] Ibid
[31] International Standard Organization, *ISO 27000: 2018 , hal 12*

sistem manajemen keamanan informasi yang didalamnya mengatur kebijakan, proses, prosedur, struktur organisasi, perangkat lunak dan perangkat keras yang memiliki pengaruh terhadap aset informasi. Sistem Manajemen Keamanan Informasi (SMKI) yang berada di dalam ISO/IEC 27001 dikembangkan untuk mengeleminir resiko yang mengancam sistem keamanan informasi, SMKI menyediakan kebijakan dan kontrol untuk mengurangi resiko yang teridentifikasi dan juga untuk menekan potensi ancaman yang sejenis. Standar ISO/IEC 27001 adalah sebuah proses pengaplikasian kontrol terhadap manajemen keamanan informasi kepada suatu organisasi untuk menekan resiko terhadap aset dan keberlangsungan organisasi (Itradat et.al, 2014).

Berikut adalah beberapa aspek kunci yang memperngaruhi keamanan informasi dari suatu organisasi :

1. Komitmen dan Dukungan dari Manajemen. Hal ini merupakan hal yang sangat penting dalam penerapan program keamanan informasi.
2. Kebijakan dan prosedur. Kerangka kerja kebijakan harus dimulai dari arahan manajemen tertinggi yang mendefinisikan pentingnya nilai aset informasi, kebutuhan dari pengamanan aset infromasi, dan pendefinisian hirarki penanganan aset informasi yang sensitif. Kebijakan keamanan informasi harus dapat mengakomodir peraturan dan regulasi, integritas, kerahasiaan, dan ketersediaan data.
3. Organisasi. Tugas dan Tanggung jawab untuk melindungi aset peribadi masing masing harus dipahami oleh semua individu. Kebijakan keamanan informasi harus menyediakan tuntunan kepada tugas dan tanggung jawab di dalam organisasi.
4. Kesadaran dan Edukasi Keamanan Informasi. Seluruh karyawan yang ada di dalam organisasi, vendor atau pihak ketiga yang bekerja sama dengan organisasi harus diberikan pelatihan rutin untuk menumbuhkan kesadaran dan kepahaman dari kebijakan keamanan informasi yang dilaksanakan oleh organisasi.
5. Pengawasan dan Penerapan. Auditor keamanan informasi yang ada di organisasi harus mengerti mengenai cara pengamanan, kerangka kerja keamanan dan isu yang berkaitan dengan keamanan

informasi termasuk penerapan keamanan informasi yang sesuai dengan peraturan dan regulasi.

6. Penanganan dan respon terhadap insiden. Insiden keamaanan sisem komputer adalah suatu kejadian yang menganggu kinerja dari sistem komputer. Insiden yang terjadi kepada sistem komputer dapat berupa hilangnya kerahasiaan informasi, gagalnya intergrasi informasi, *denial of service*, akses berbahaya kepada system (CISA Review Manual, 2001).

Standar ISO/IEC 27001 sendiri memiliki 14 poin pembahasan, dan berdasarkan hasil observasi di Pushansiber hanya 2 poin pembahasan yang memiliki *maturity level* 3, kemudian ada 7 poin pembahasan yang ada di *maturity level* 2 dan dan ada 4 yang berada di *maturity level* 1. Untuk poin pembahasan mengenai hubungan dengan supplier dianggap tidak dipergunakan dikarenakan hingga saat ini pengadaan sarana dilakukan oleh Pushansiber.

Dalam pelaksanaan harian hanya berupa SOP harian dan Laporan yang belum semuanya dibukukan menjadi sebuah kebijakan dan peraturan yang dipatuhi, dijalankan dan diawasi bersama. Seharusnya dengan adanya komitmen dan dukungan dari manajemen dapat melahirkan sebuah kebijakan dan prosedur yang harus dilaksanakan dan dipatuhi oleh semua pihak yang berada di lingkungan Pushansiber, baik itu manajemen, karyawan, tamu, hingga supplier. Pushansiber sebagai sebuah organisasi yang bertugas untuk melindungi kementerian pertahanan dari serangan luar seharusnya lebih ketat dalam menjalankan peraturan terkait keamanan informasi.

Larangan untuk membawa handphone sudah dibuat namun belum dijalankan oleh manajemen maupun personel yang berada di lingkungan Pushansiber. Seharusnya larangan ini menjadi perhatian bagi seluruh *stakeholder* yang beraktifitas di lingkungan Pushansiber. Lalu kaitannya dengan penyaringan dan perjanjian untuk personel masih diurus oleh biro kepegawaian Kementerian Pertahanan, hal ini dapat menjadi celah keamanan bagi Pushansiber dimasa yang akan datang. Seharusnya seluruh prosedur pengamanan seperti *background checking* personel dilakukan oleh Pushansiber. Hal ini melanggar konsep kerahasiaan dan integritas dalam sistem manajemen keamanan informasi

Walau edukasi keamanan informasi sudah dilakukan, namun belum adanya sebuah peraturan yang mengikat dan dapat memberikan hukuman bagi personel yang melakukan pelanggaran. Seharusnya Pushansiber menjaga dengan sangat ketat keamanan informasi yang dimiliki. Pushansiber juga belum mengatur perihal prosedur penanganan segala bentuk media yang sedang maupun sudah tidak terpakai. Pushansiber belum mengatur pelarangan untuk memakai media penyimpanan pribadi di lingkungan Pushansiber, dan belum ada peraturan untuk memusnahkan media penyimpanan yang sudah terpakai. Seharusnya Pushansiber memiliki sebuah prosedur dalam larangan penggunakan media penyimpanan potable dan pemusnahan media penyimpanan yang sudah tidak terpakai untuk menghindari adanya kebocoran atau penggunaan informasi oleh pihak yang tidak berkepentingan. Hal ini tidak mencerminkan kerahasiaan yang diatur oleh sistem manajemen keamanan informasi.

Pada pelaksanaannnya pengiriman pesan dan data digital telah dilakukan dengan menggunakan berbagai macam aplikasi internal yang dimiliki Kementerian Pertahanan, namun didalam SMKI hal ini belumlah cukup. Harus terdapat sebuat aturan yang tertulis dan terdokumentasi yang mengatur pertukaran informasi yang terkait dengan Pushansiber dan Kementerian Pertahanan. Selanjutnya dalam pengaturan log akses, Pushansiber masih belum memiliki kontrol terhadap hal tersebut dikarenakan belum adanya sarana berupa sistem yang dapat mengelola log yang dapat menjadi panduan utama apabila terdapat serangan yang mengarah ke Kementerian Pertahanan. Lalu didalam hal *development* sendiri Pushansiber masih terbentur dengan penganggaran.

Dari semua hasil Analisa data observasi yang menggunakan Standar Sistem Manajemen Keamanan Informasi ISO/IEC 27001, Pushansiber masih dapat dikatakaan jauh dari *maturity level* ideal yaitu 5. Dari hasil observasi tersebut menemukan bahwa Pushansiber sebagian besar berada di *maturity level 2* yaitu sudah ada penanganan secara teknis namun belum di dokumentasikan secara benar yang kemudian disusun menjadi sebuah kebijakan atau aturan yang menjaga keamana informasi di lingkungan Pushansiber. Berdasarkan data yang diperoleh dari hasil observasi dan wawancara dengan nasarasumber di

Pushansiber dapat disimpulkan bahwa Sistem Manajemen Keamanan Informasi yang ada di Pushansiber masih tergolong tidak aman. Berbagai macam hal tersebut selalu terbentur dengan tidak adanya anggaran untuk membangun keamanan informasi di lingkungan Pushansiber.

Hasil penelitian ini juga sejalan dengan penelitian yang dilakukan oleh Awni Itradad, dkk (2014) yang menemukan sistem informasi Universitas Hashemite memiliki tingkat kerawanan yang sangat tinggi, dinilai dari banyaknya jumlah dan jenis celah keamanan yang dapat menjadi peluang untuk melumpuhkan sistem keamanan informasi universitas tersebut. Dalam penelitian ini menemukan banyak celah keamanan informasi di Pushansiber yang juga menggunakan ISO/IEC 27001 sebagai alat ukur. Dengan menggunakan standar tersebut dapat dilakukan asesmen terhadap keamanan informasi di organisasi.

Hambatan dalam Penerapan Keamanan Informasi di Pushansiber.

Keamanan informasi adalah sesuatu yang memastikan informasi yang ada di dalam perusahaan dilindungi dari pengungkapan kepada pengguna yang tidak memiliki otoritas (Kerahasiaan), dari modifikasi yang salah (Integritas) dan kegagalan akses saat informasi tersebut dibutuhkan (Ketersediaan) (ISACA, COBIT 5, 2012). Didalam CISA Review Manual (2012) menjelaskan bahwa komitmen dan dukungan dari manajemen, kebijakan dan prosedur, organisasi, kesadaran dan edukasi keamanan informasi, pengawasan dan penerapan serta penanganan dan respon insiden menjadi beberapa aspek kunci yang mempengaruhi keamanan informasi di dalam suatu organsiasi. Dari Subbab sebelumnya telah ditemukan bahwa Pushansiber belum memiliki keamanan informasi yang memadai, beberapa poin pembahasan dari ISO/IEC 27001 yang sangat rentan dimiliki Pushansiber adalah pengaturan supplier, pengembangan sistem dan kebijakan keamanan informasi. Pushansiber merupakan sebuah organisasi yang pada tahun 2017 lahir dari COC (*Cyber Operation Center*) Pusdatin.

Berdasarkan hasil wawancara dan hasil studi pustaka yang telah peneliti lakukan, maka peneliti menyimpulkan bahwa aspek penting yang menjadi hambatan dalam penerapan keamanan informasi di Pushansiber adalah belum adanya kebijakan dalam skala kementrian yang dapat menjadi payung hukum dan rujukan untuk Pushansiber membuat

sebuah kebijakan internal organisasi, dimana kebijakan keamanan informasi berada didalamnya. Selama ini Pushansiber belum dapat membuat kebijakan internal dalam hal ini SOP dan penganggaran untuk membentuk keamanan informasi dikarenakan acuan kebijakan setingkat kementrian belum ada.

Penelitian ini menemukan bahwa Pushansiber sebagai sebuah satker yang berada di lingkungan Kementerian Pertahanan dengan tugas penyusunan, pelaksanaan, dan pemantauan dalam penjaminan keamanan pertahanan siber di lingkungan Kementerian Pertahanan. Pushansiber merupakan pemekaran dari unit COC (*Cybre Operation Center*) yang sebelumnya berada dibawah Pusdatin.

Pemekaran ini terjadi pada tahun 2017 sebagai upaya untuk mengurangi beban yang ada di Pusdatin. Pushansiber terbentuk namun belum ada Permenhan yang mengatur hal tersebut hingga terbitlah Permenhan no. 14 Tahun 2019. Selama 2 tahun tersebut Pushansiber tidak bisa mengajukan penganggaran dikarenakan secara teknis sudah pisah dengan Pusdatin namun belum ada Permenhan yang menjadi landasan untuk mengajukan anggaran ke Bainstrahan sebagai induk baru dari satker ini.

Hambatan yang timbul akibat hal tersebut tidak hanya pada sisi penganggaran saja. Secara teknis yang sebelumnya Pushansiber mengikuti kebijakan keamanan informasi yang ada di Pusdati yang dalam hal ini sudah lebih *mature* dengan sudah mennerepkan standar sistem manajemen keamanan informasi ISO/IEC 27001. Sehingga dalam kesehariannya Pushansiber hanya menjalankan SOP yang diatur secara teknis harian dikarenakan belum adanya sebuah kebijakan organisasi yang merupakan turunan dari kebijakan pertahanan yang berlandaskan dari Peraturan Menteri Pertahanan. Hal ini dapat dimaknai sebagai ketidaksinkronan kebijakan. Hambatan yang dimiliki oleh Pushansiber bertentangan dengan aspek kunci pengamanan informasi oleh ISACA (2001) yaitu belum adanya kebijakan dan prosedur yang mendukung keamanan informasi di lingkungan Pushansiber.

Hasil penelitian ini mendukung penelitian sebelumnya oleh Haryanto (2015) yang menyimpulkan pengelolaan keamanan informasi harus memperhatikan pihak internal dan eksternal yang memiliki kaitan dengan organisasi dengan memperhatikan klausul keamanan informasi dengan pihak terkait. Dalam penelitian ini menemukan

belum adanya kebijakan pada tingkat Kementrian dalam hal ini Kementrian Pertahanan yang dapat menjadi acuan dalam pembuatan kebijakan internal keamanan informasi di Pushansiber, dalam hal ini pihak eksternal organisasi yaitu Kementrian Pertahanan selaku induk dari organisasi Pushansiber memiliki pengaruh terhadap keamanan informasi di Pushansiber. Dengan adanya Permenhan No.14 Tahun 2019 dapat menjadi solusi bagi hambatan penerapan keamanan informasi di Pushansiber. Dengan adanya Permenhan tersebut, Pushansiber dapat membuat kebijakan internal organisasi yang dimana kebijakan keamanan informasi juga berada didalamnya, serta mengajukan anggaran untuk kajian terkait pembuatan kebijakan internal tersebut.

Strategi ISO/IEC 27001: 2013 sebagai Strategi Keamanan Informasi di Pushansiber Kementerian Pertahanan.

Keamanan informasi adalah sesuatu yang memastikan informasi yang ada di dalam perusahaan dilindungi dari pengungkapan kepada pengguna yang tidak memiliki otoritas (Kerahasiaan), dari modifikasi yang salah (Integritas) dan kegagalan akses saat informasi tersebut dibutuhkan (Ketersediaan) (ISACA, COBIT 5, 2012). Pushansiber selaku pengelola keamanan informasi di Kementerian Pertahanan dalam rangka pertahanan siber harus memiliki kemampuan untuk mengamankan informasi internal organisasi. Maka dibutuhkan sebuah perencanaan dala upaya mendukung pelaksanaan pengamanan jaringan di Kementerian Pertahanan yang merupakan tugas utama dari Pushansiber.

Dari hasil wawancara dapat ditarik kesimpulan bahwa *Ends* yaitu sebuah tujuan atau dari Pushansiber adalah melakukan pemantauan dan pengamanan luar dari jaringan Kementerian Pertahanan yang berhubungan langsung dengan internet. Hal ini dilakukan dengan melakukan pemantauan terhadap *traffic* akses yang masuk ke Kementerian Pertahanan.

Means atau sarana yang dimiliki oleh Pushansiber untuk menuju *Ends* nya adalah adanya sensor di beberapa titik yang mampu mendeteksi *traffic* yang menuju atau keluar dari Pushansiber. Kemudian apabila ada sebuah anomali maka diperlukan analisa dengan menggunakan sumber daya yang dimiliki oleh Pushansiber, baik itu sumber daya teknis maupun sumber daya manusia.

Dari hasil wawancara juga dapat dijelaskan bahwa *ways* dari usaha dalam mencapai *Ends* dari Pushansiber masih memiliki banyak masalah, diantaranya adalah adanya *remote* akses oleh vendor, belum adanya kebijakan internal organisasi, keterbatasan anggaran serta kurangnya edukasi keamanan informasi pada personel Pushansiber.

Penelitian ini menggunakan Sistem Manajemen Keamanan Informasi sebagai Strategi dalam Pertahanan pada umumnya dan Keamanan Informasi pada khususnya. Strategi terdiri dari Ends, Means dan Ways, yang dianalisa dalam penelitian ini sebagai berikut:

Ends. Merupakan tujuan yang menjadi sasaran. *Ends* dalam penelitian ini adalah lancarnya tugas dari Pushansiber yaitu melakukan pengamanan luar jaringan Kementerian Pertahanan dengan melkukan pemantauan terhadap *traffic digital* yang masuk dan keluar Kementerian pertahanan. Sesuai dengan PERMENHAN no 14 tahun 2019, dimana Pushansiber sebagai salah satu badan yang melakukan pengamanan di lingkungan Kementerian Pertahanan, khususnya pada instalasi strategis Kementerian Pertahanan.

Means. Adalah sumber, sarana dan prasarana yang digunakan dalam mencapai tujuan. Sensor jaringan dan Sumber Daya Manusia yang dimiliki Pushansiber menjadi means utama dalam strategi ini.

Ways. Adalah cara yang ditempuh untuk mencapai tujuan. Penelitian ini menemukan bahwa dalam pelaksanaan harian untuk melaksanakan tugasnya, Pushansiber masih memiliki banyak kendala. Salah satunya adalah adanya *remote* akses oleh vendor, kebijakan internal organisasi, dan keterbatasan anggaran dalam penerapan keamanan informasi.

Solusi untuk masalah tersebut adalah dengan melakukan asesmen sistem manajemen keamanan informasi dengan ISO/IEC 27001. Dari 14 poin pembahasan, beberapa diantaranya adalah mendefinisikan masalah mengenai pengaturan keamanan informasi yang berkaitan dengan vendor, kebijakan dan pengorganisasian keamanan informasi sera aspek keberlangsungan keamanan informasi. Poin kontrol yang ada didalamnya dapat menjadi rujukan yang perlu ditingkatkan dalam mengatasi hambatan yang ditemukan dalam penelitian ini.

Maka dapat disimpulkan bahwa asesmen sistem manajemen keamanan informasi dengan berdasar kepada ISOIEC 27001, dan dengan *maturity level* dari ISACA dapat menjadi rujukan dalam melakukan asesmen keamanan informasi dalam mengidentifikasi celah keamanan informasi di lingkungan organisasi dan menjadi landasan teknsi dalam membangun sistem manajemen keamanan informasi di Pushansiber.

Kesimpulan, Rekomendasi dan Batasan

Berdasarkan hasil pembahasan dan pengolahan data yang peneliti lakukan maka dapat disimpulkan hal-hal sebagai berikut.

1. Adapun pengelolaan keamanan informasi yang ada di Pushansiber yang diukur dengan ISO 27001 masih berada didalam zona tidak aman dikarenakan hanya ada 2 poin pembahasan yang memiliki *maturity level* 3 yang artinya hanya kedua poin tersebut yaitu pengorganisasian keamanan informasi dan aspek keberlangsungan keamanan informasi yang sudah memiliki pedoman tertulis sebagai kontrol yang terdokumentasi. Kemudian terdapat 7 poin pembahasan yang memiliki *maturity level* 2 yaitu sudah adanya kontrol yang dilakukan secara teknis namun belum terdokumentasikan menjadi sebuah pedoman yang di sepakati dan dipatuhi bersama. Bahkan masih ada 4 poin pembahasan yang berada di *maturity level* 1 yaitu adanya masalah yang timbul namun belum ada control yang dilakukan oleh Pushansiber, hanya penyelesaian secara langsung secara *adhoc* yang dimana hal ini menjadi potensi masalah yang akan timbul dikemudian hari apabila tidak dibuat sebuah petunjuk teknis yang terdokumentasi secara lengkap dan diakui bersama.
2. Hambatan utama yang ada di dalam Pushansiber dalam usaha pengembangan keamana informasi sehingga mendapatkan penilaian buruk yang diukur dengan standar SMKI ISO/IEC 27001 adalah belum adanya kebijakan berupa Permenhan yang menjadi landasan bagi Pushansiber dalam merencanakan berbagai macam usaha dalam membentuk keamanan informasi di lingkungan Pushansiber. Sehingga dari tahun 2017 hingga akhirnya diterbitkan

Permenhan no.14 Tahun 2019, Pushansiber mengalami sebuah kendala yaitu tidak sinkronnya kebijakan dan pelaksanaan teknis yang mengakibatkan Pushansiber sangat buruk dalam melaksanakan pengelolaan keamanan informasi di lingkungan internal Pushansiber yang kemudian pada akhirnya akan mengganggu dan membatasi kinerja Pushansiber dalam upaya pengelolaan pertahanan siber di lingkungan Kementerian Pertahanan.

3. Sistem manajemen keamanan informasi ISO/IEC 27001 dinilai dapat menjadi strategi keamanan informasi di Pushansiber dengan menjadi salah satu dari Ways dengan poin poin kontrol yang dibedah jelas dalam standar ini dapat menjadi rujukan dalam penilaian dan pengembangan sarana (Means) yang dimiliki oleh Pushansiber dalam tugas hariannya yaitu pengelolaan pertahanan siber di lingkungan Kementerian Pertahanan (Ends).

Penelitian ini juga merumuskan sebuah strategi untuk Pushansiber dalam membangun keamanan informasi di lingkungan Pushansiber. Dengan hasil observasi yang dilakukan saat ini menemukan bahwa keamanan informasi di Pushansiber yang dianalisa dengan standar sistem manajemen keamanan informasi ISO/IEC 27001 masih berada di bawah *maturity level* 3. Maka saran praktis dalam penelitian ini merumuskan sebuah strategi 5 tahun untuk membangun keamanan informasi di Pushansiber yang dirumuskan sebagai berikut:

1. Pada tahun pertama, keamanan informasi dibangun dengan berlandaskan kepada temuan dari hasil observasi pada penelitian ini. Target pada tahun pertama adalah mempersiapkan Pushansiber untuk dilakukan penilaian kembali dnegan standar SMKI ISO/IEC 27001 di tahun ke 2.
2. Pada tahun kedua, dilakukan penilaian kembali keamanan informasi di Pushansiber dengan ISO/IEC 27001 untuk melihat perkembangan dari keamanan informasi di Pushansiber. Target dari tahun ke dua adalah *maturity level* 3, dengan merumuskan semua kebijakan dan peraturan yang mengatur keamanan informasi

dengan bardasar kepada poin pembahasan di ISO/IEC 27001. Bila ada temuan maka digunakan sebagai acuan untuk evaluasi di tahun berikutnya.

3. Pada tahun ketiga, dipersiapkan sebuah divisi atau tim yang bertugas untuk menjaga implementasi ISO/IEC 27001 di Pushansiber. Tim ini juga bertugas untuk melakukan audit tahunan di Pushansiber secara keseluruhan dengan standar ISO/IEC 27001 sebagai acuan. Target pada tahun ketiga adalah Pushansiber memiliki *maturity level* 4 dalam sistem manajemen keamanan informasi.
4. Pada tahun keempat, juga dilakukan penilaian tahunan sistem manajemen keamanan informasi ISO/IEC 27001 untuk melihat konsistensi implementasi SMKI di Pushansiber. Apabila pada tahun ini mendapatkan *maturity level* 4, maka dipersiapkan juga kebijakan, sumberdaya manusia dan peraturan untuk mencapai *maturity level* 5 ditahun berikutnya.
5. Pada tahun kelima, penilaian juga dilakukan untuk melihat implementasi SMKI di Pushansiber. Apabila *maturity level* masih belum mencapai 5, maka diadakan evaluasi kembali. Namun apabila *maturity level* sudah berada di *level* 5, untuk tahun tahun berikutnya tetap dilakukan penilaian tahunan SMKI 27001 sebagai upaya *maintenance* keamanan informasi di Pushansiber.

Sebagai batasan, penelitian ini menggunakan kerangka ISO/IEC 27001: 2013 dan Maturity Level dari ISACA dalam menilai keamanan informasi yang ada di Pushansiber Kementerian Pertahanan Republik Indonesia di akhir tahun 2019.

Daftar Pustaka

Buku

Creswell, J. (2007). *Qualitative Inquiry & Research Design : Choosing Among Five Approaches.* Thousand Oaks: Sage Publication.

Patton, M. (2015). *Qualitative Research & Evaluation Method.* USA: Sage.

Satori, D., & Komariah, A. (2011). *Metode Penelitian Kualitatif.* Bandung: Alfabeta.

Sugiyono. (2009). *Kualitatif dan R&D.* Bandung: Alfabeta.

Artikel Jurnal

Nasser, A. (2017). Information security gap analysis based on ISO 27001:2013 standard : A case study of yhe Yemeni Academy for Graduate Studies, Sana's, Yemen. *International Journal of Science research in Multidisciplinary Studies*, 4-13.

Dokumen

International Standard Organization. (2018). *ISO/IEC 27000: 2008*

International Standard Organization. (2013). *ISO/IEC 27001: 2013*

Kementerian Pertahanan Republik Indonesia. (2014). *Permen No. 82 Tahun 2014, Tentang Pedoman Pertahanan Siber.* Jakarta: Kementerian Pertahanan Republik Indonesia.

Website

Antara News. (2010, September 28). *Apa itu Stuxnet ?* Retrieved from Antara News : https://www.antaranews.com/berita/222505/apa-itu-stuxnet. Diakses pada 13 Oktober 2019.

Kementerian Pertahanan. (n.d.). *Kementerian Pertahanan Republik Indonesia*. Retrieved from Pusat Data dan Informasi: https://www.kemhan.go.id/pusdatin/faq

Kompas Tekno. (2010, Oktober 04). *34.000 Komputer di Indonesia Terinfeksi Stuxnet*. Retrieved from Kompas Tekno: https://tekno.kompas.com/read/2010/10/04/23074744/34.000.komputer.di.indonesia.terinfeksi.stuxnet. Diakses pada 1 Oktober 2019.

Tempo.co. (2013, Maret 1). *Virus Stuxnet untuk Melumpuhkan Nuklir Iran*. Retrieved from TEMPO.CO: https://dunia.tempo.co/read/464583/virus-stuxnet-untuk-melumpuhkan-nuklir-iran/full&view=ok. Diakses pada 13 Oktober 2019.