LOGIC: Jurnal Penelitian Informatika
Vol. 1, Issue 1, pp. 59–66 (2023)
doi: http://doi.org/10.25124/logic.v1i1.6463

RESEARCH ARTICLE

Analisis Manajemen Keamanan Informasi Dengan Menggunakan Kontrol Iso 27002:2013 Pada Pemerintah Kota Ambon (Studi Kasus Pada Bagian Dinas Komunikasi Dan Informatika Kota Ambon)

Antonio Bennarivo Pattiradjawane, Farisya Setiadi* and Rio Guntur Utomo

Fakultas Informatika, Universitas Telkom, Bandung, 40257, Jawa Barat, Indonesia
*Corresponding author: farisyasetiadi@telkomuniversity.ac.id2
Received on 06 August 2023; accepted on 30 August 2023

Abstrak

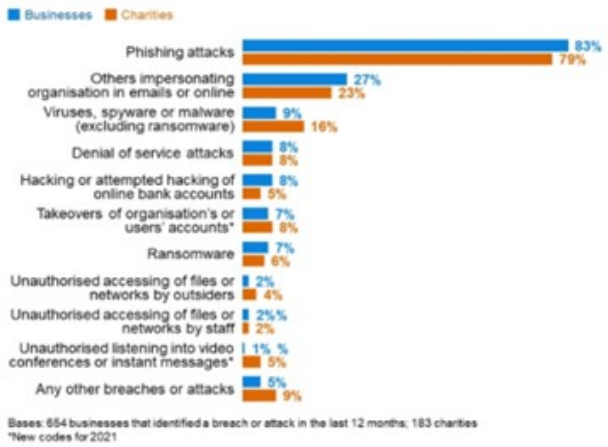
Informasi merupakan suatu aset berharga yang harus dilindungi baik secara individu atau organisasi. Oleh sebab itu dibutuhkan suatu perlindungan atau keamanan informasi yang bisa meminimalisir terhadap ketidakbenaran atau keancaman informasi itu sendiri. Berdasarkan regulasi atau aturan yang telah dikeluarkan oleh pihak yang berwenang, salah satunya Peraturan Menteri Kominfo No 4 Tahun 2016 Pasal 7, yang mewajibkan setiap penyelenggaraan sistem elektronik harus bisa menerapkan keamanan informasi sesuai dengan standar yang telah ditetapkan. Oleh karena itu, berdasarkan regulasi di atas, maka peneliti melakukan penelitian terhadap objek penelitian yakni Dinas Komunikasi dan Informatika Pemerintah kota Ambon yang mana penelitian menggunakan metode kualitatif dengan pengumpulan dan validasi data secara wawancara, observasi serta kuesioner, analisis data menggunakan *gap analysis* dan mengukur tingkat kematangan dengan indeks CMMI serta penambahan kriteria dengan meninjau Permenpan 59 Tahun 2020. Hasil penelitian menunjukan bahwa tingkat kematangan dari objek penelitian berada pada nilai 1,84 dan berada pada posisi (*repeteable*) itu berarti Dinas Komunikasi dan Informatika Pemerintah Kota Ambon masih melakukan prosedur atau kebijakan secara sebagian atau belum menyeluruh atau dengan kata lain Terdapat proses yang telah dilakukan tetapi belum didokumentasikan atau belum sesuai dengan prosedur yang berlaku.

Key words: Keamanan Informasi, Dinas Komunikasi dan Informatika, Iso 27002:2013, Permenkominfo, Permenpan, CMMI.

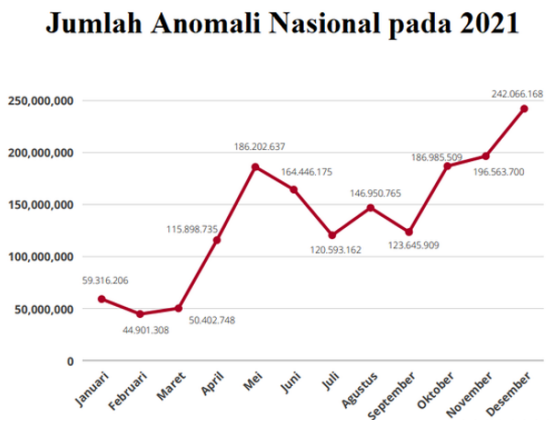
Pendahuluan

Revolusi Industri 4.0 merupakan suatu era yang mana hampir semua aspek kehidupan memerlukan teknologi dan informasi dalam implementasinya. Menurut (Haag dan Keen,1996) [1] manusia dalam melakukan pekerjaan dan tugas-tugasnya yang berhubungan dengan informasi atau pesan harus bisa menggunakan teknologi informasi sebagai sarana untuk menunjang pekerjaannya. Oleh sebab itu, teknologi informasi merupakan suatu hal mutlak yang diperlukan dalam menunjang kehidupan manusia di era revolusi industri 4.0 salah satunya berpengaruh di bidang pemerintahan contohnya seperti *E-Government* (Pemerintahan Elektronik) yang didasarkan pada dasar hukum Perpres No 95 Tahun 2018. Selain itu juga, ada beberapa peraturan perundang-undangan yang dibuat berkaitan dengan keamanan informasi. contohnya seperti Perpres No 95 Tahun 2018 yang mengatur tentang SPBE (Sistem Pemerintahan Berbasis Elektronik), Peraturan Menteri Komunikasi dan Informatika No 4 Tahun 2016 Pasal 1 Ayat 5 dan 6 yang mana pasal 5 mengatur tentang sistem manajemen pengamanan informasi, dan pasal 6 yang mengatur tentang aspek-aspek keamanan informasi (CIA) dan Peraturan Menteri Komunikasi dan Informatika No 4 Tahun 2016 Pasal 4 tentang Kategorisasi Sistem Elektronik berdasarkan asas risiko. beberapa peraturan ini dikeluarkan untuk mengatur keamanan informasi pada bidang pemerintahan.

Menurut G.J.Sismsons, Keamanan Informasi adalah bagaimana kita dapat mencegah penipuan (*cheating*) atau paling tidak mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi,di mana informasinya itu sendiri tidak memiliki arti fisik sehingga rentan terhadap penipuan yang terjadi pada sistem berbasis informasi itu sendiri, sehingga diperlukan manajemen keamanan informasi yang baik untuk mencegah adanya ancaman yang terjadi pada informasi yang dimiliki. Ancaman Keamanan informasi merupakan suatu kejadian yang bisa merugikan suatu pihak dikarenakan adanya kehilangan data dan informasi yang berharga. Ancaman keamanan informasi ini sendiri bisa terjadi di mana saja dan kapan saja baik secara nasional maupun internasional. Berikut ini merupakan contoh kasus keamanan informasi yang terjadi di dunia (*internasional) dan Indonesia (Nasional). Berdasarkan hasil survei pada gambar 1 maka bisa dilihat bahwa terjadi banyak serangan yang menyerang keamanan informasi. Phising attacks* merupakan tipe ancaman yang paling besar persentasenya. Selain itu ada juga tipe ancaman seperti *other impersonating organization,*



Gambar 1. Survey Tipe Ancaman Keamanan Informasi Tahun 2021 di Dunia.



Gambar 2. Hasil Survey Ancaman Keamanan Informasi di Indonesia Tahun 2021.

virus or malware, hacking, ransomware, dan lain-lain. Tipe ancaman ini bisa terjadi dikarenakan faktor manajemen keamanan informasi yang diterapkan belum berdasarkan dengan standar yang berlaku, sehingga informasi yang dimiliki belum terjamin keamanannya dan bisa mendapatkan ancaman keamanan informasi.

Selain ancaman yang terjadi di seluruh dunia, Indonesia juga menjadi salah satu negara yang tidak terlepas dari ancaman keamanan informasi itu sendiri. Oleh sebab itu pemerintah membentuk sebuah badan yang disebut dengan BSSN (Badan Siber dan Sandi Negara) yang merupakan sebuah lembaga yang bergerak di bidang keamanan informasi tentang siber dan persandiaan yang mempunyai tugas pokok untuk mengatur, mengkoordinasikan dan menyelenggarakan pengamanan berita rahasia negara yang dikirim melalui sarana komunikasi antara aparatur negara di seluruh Indonesia. Berdasarkan data laporan Tahunan "Monitoring Keamanan Siber" BSSN 2021 di atas 2 bisa dilihat bahwa ancaman keamanan informasi yang terjadi pada bulan Januari – Desember 2021 berjumlah 1,6 miliar atau tepatnya 1.637.973.022 anomali trafik atau serangan siber (*cyber attack*) yang terjadi di seluruh wilayah Indonesia sepanjang tahun 2021.

Selain itu, ancaman keamanan informasi juga pernah terjadi di Dinas Komunikasi dan Informatika Pemerintah Kota Ambon. Dan berdasarkan hasil wawancara yang telah dilakukan, didapatkan bahwa objek penelitian juga pernah mengalami ancaman keamanan informasi seperti *hacking*, *serverdown* yang terjadi hampir di setiap tahun, upaya pembobolan data instansi oleh pihak yang tidak bertanggung jawab pada tahun 2020 hal ini terjadi karena keamanan fisik yang dimiliki oleh objek penelitian belum optimal.

Berdasarkan data yang ada maka analisis keamanan informasi akan dilakukan untuk mengatasi permasalahan yang terjadi di Dinas Komunikasi dan Informatika Pemerintah Kota Ambon untuk mengetahui bukti apa saja yang dimiliki oleh objek penelitian serta menganalisis sistem manajemen keamanan informasi menggunakan *gap analysis* dan menentukan *maturity level* dari keamanan informasi yang dimiliki untuk digunakan sebagai acuan informasi pada Dinas Komunikasi dan Informatika Kota Ambon sebagai tujuan utama.

Tinjauan Pustaka

Landasan Teori

Terdapat beberapa Landasan Teori yang digunakan dalam penelitian ini antara lain seperti definisi keamanan informasi,sistem manajemen keamanan informasi, studi literatur serta jenis-jenis pengumpulan data.

Keamanan Informasi

Keamanan informasi merupakan suatu perlindungan terhadap informasi yang mana di dalamnya terdapat sistem dan perangkat yang digunakan untuk melindungi keamanan informasi tersebut. Menurut (Whitman dan Mattord,2011) [2], keamanan informasi yang bisa ditinjau keamanannya, yaitu:

a. Keamanan fisik
b. Keamanan pribadi
c. Keamanan operasional
d. Keamanan komunikasi
e. Keamanan jaringan

Aspek-aspek Keamanan Informasi

Terdapat 3 Aspek Keamanan informasi yang sangat penting dan biasanya disingkat dengan CIA yang mempunyai arti *Confidentiallity, Integrity, Availibillity.*

Sistem Manajemen Keamanan Informasi

Sistem manajemen keamanan informasi adalah sebuah sistem yang dirancang khusus dalam sebuah organisasi dengan tujuan untuk mengamankan dan melindungi informasi yang dimiliki oleh organisasi itu sendiri. SMKI ini juga mempunyai beberapa *framework* yang bisa digunakan antara lain COBIT 5.0, NIST 800-53, ISO 27001, dan lain sebagainya. namun, pada penelitian ini menggunakan ISO 27002:2013 sebagai *framework* dalam menganalisis permasalahan yang sedang terjadi.

Standar ISO 27002:2013

ISO 27002:2013 adalah suatu standar keamanan informasi yang diterbitkan oleh *The International Organization for Standarization* (ISO) dan *The International Electrotechnical Commision* (IEC), yang berjudul teknologi informasi. ISO 27002:2013 mengatur tentang sistem manajemen keamanan informasi (SMKI) menggunakan 14 area pengamanan dengan setiap area mempunyai fungsi kontrolnya masing-masing.

Capability Maturity Model for Integration

Pada penelitian ini, peneliti mengacu pada tingkat kematangan dengan menggunakan CMMI (*Capability Maturity Model for Integration*). Yang mana menurut Komalasari dan Perdana (2014) mengungkapkan bahwa "CMMI adalah model kematangan yang digunakan untuk melakukan penilaian manajemen TI secara lebih efisien yang dapat diterapkan atau diimplementasikan ke masing-masing klausul ISO 27002:2013.

Table 1. Definisi Urutan Tingkat CMMI

Indeks Kematangan	Definisi
0 *Non Existent*	Merupakan nilai yang paling kecil yang mana perusahaan tidak mengetahui ada masalah yang terjadi dan harus diatasi sehingga bersifat kurang secara menyeluruh terhadap proses yang dapat dikenali.
1 *Initial*	Merupakan nilai dengan tingkat keamanan informasi yang tidak matang.ini reaktif, artinya memiliki prosedur tertulis yang buruk dan proses yang tidak dapat diprediksi yang memiliki hasil yang tidak pasti. Pada level ini mungkin memiliki keahlian keamanan informasi yang terbatas, dengan pengetahuan strategi atau taktik yang terbatas dalam menghadapi ancaman.
2 *Repeteable*	Merupakan nilai yang masih mempertahankan sifat reaktif, tetapi organisasi di level ini lebih terorganisir dalam proyek terkait keamanan informasi. Terdapat proses yang telah dilakukan tetapi belum didokumentasikan atau belum sesuai dengan prosedur yang berlaku.
3 *Defined*	Merupakan nilai yang lebih baik dari level sebelumnya. pada level ini organisasi cenderung menjadi proaktif dalam pendekatannya terhadap insiden keamanan informasi. Para stakeholder lebih bisa menyesuaikan proses mereka dengan standar yang jelas yang sejalan dengan tujuan bisnis organisasi.
4 Managed	Merupakan nilai yang Dikelola Secara Kuantitatif berarti bahwa organisasi telah mencapai tingkat kematangan di mana proses, proyek, dan kemampuan terukur didefinisikan dan dikendalikan dengan jelas. Lingkungan ini memerlukan tim keamanan informasi yang berpengalaman dengan kepemimpinan yang kuat, anggaran yang baik, dukungan dari pihak yang berwenang dan lebih tinggi.
5 Optimized	Merupakan nilai yang pada dasarnya membangun apa yang saat ini ada sebagai organisasi yang matang, kuantitatif, dan kualitatif. Namun, hanya sedikit organisasi yang dapat mencapai tingkat tertinggi ini karena kurangnya keahlian, kumpulan bakat yang terbatas, anggaran yang terbatas, dan kurangnya dukungan manajemen. Semua ini menghambat kemajuan menuju terciptnya keamanan informasi yang baik dalam sebuah organisasi.

Penerapan Tingkat Keamanan Informasi yang diterapkan oleh organisasi didasarkan pada model tingkat kematangan level yang dimulai dari nilai 0 sampai dengan nilai 5 dengan maksud untuk mengetahui keberadaan dari permasalahan yang ada serta menentukan prioritas peningkatan. untuk kematangan CMMI secara umum sebagai berikut: 1. Berdasarkan nilai dari Level Kematangan maka dapat dikelompokan sebagai berikut: 2

Table 2. Pengelompokan Tingkatan CMMI

Indeks Kematangan	Level Kematangan
0.00-0.50	*0-Non-Existent*
0.51-1.50	1 *Initial*
1.51-2.50	2 *Repetable*
2.51-3.50	3 *Defined*
3.51-4.50	4 Managed
4.51-5.00	5 Optimized

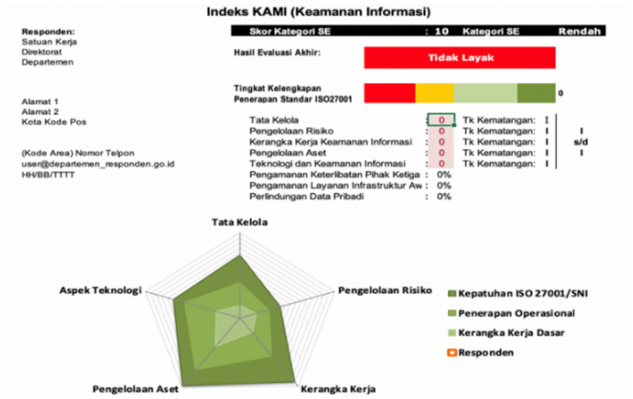
Sistem Pemerintahan Berbasis Elektronik (SPBE)

Sistem pemerintahan berbasis elektronik adalah penyelenggaraan pemerintahan yang memanfaatkan TIK untuk memberikan layanan kepada pengguna SPBE dan diatur dalam Peraturan Presiden No 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. SPBE ini ditujukan untuk mewujudkan tata kelola pemerintahan yang bersih, akuntabel, efektif dan transparan. Berikut ini merupakan visi misi, tujuan dan sasaran dari SPBE 3.

Indeks KAMI

Indeks KAMI adalah suatu alat evaluasi yang digunakan untuk menganalisis suatu tingkat keamanan informasi di dalam suatu organisasi

Gambar 3. Visi Misi, Tujuan dan Sasaran dari SPBE.



Gambar 4. Dashboard Indeks KAMI.

berdasarkan pada kriteria ISO/IEC 27001:2013. Berikut ini merupakan Dashboard Indeks KAMI 4.

Regulasi Manajemen Keamanan Informasi

Regulasi manajemen keamanan informasi merupakan suatu aturan yang dikeluarkan oleh pemerintah untuk mengatur tentang keamanan informasi. Terdapat beberapa regulasi yang dikeluarkan oleh pemerintah antara lain PerPres No 95 Tahun 2018, Permenpan No 59 Tahun 2020 & Permen Kominfo No 4 Tahun 2016.

Pengumpulan Data

Data merupakan hal inti yang diperlukan dalam sebuah penelitian dan untuk memperoleh data yang dibutuhkan maka diperlukan pengumpulan data yang bisa dilakukan dengan berbagai teknik. Pengumpulan data yang baik dengan teknik yang benar akan berpengaruh terhadap hasil penelitian yang dilakukan sehingga dalam proses pengumpulan data harus dilakukan dengan teknik yang baik dan benar. Terdapat dua metode pengumpulan data yakni kualitatif dan kuantitatif. Secara umum terdapat lima metode pengumpulan data kualitatif yakni Wawancara Observasi, Kuesioner, Dokumentasi dan *Focus Grup Discusion* (FGD).

ANNEX					
ANNEX A	KONTROL	KONDISI	EVALUASI	REKOMENDASI	NILAI KONTROL OBJEKTIF
5	KEBIJAKAN KEAMANAN INFORMASI				
5.1.	ARAHAN MANAJEMEN UNTUK KEAMANAN INFORMASI				
	OBJECTIVE *to provide management direction and support for information security in accordance with bussines requirements and relevant laws and regulations* Untuk memberikan arah dan dukungan manajemen untuk keamanan informasi sesuai dengan persyaratan bisnis dan regulasi dan hukum yang relevan				
5.1.1	KEBIJAKAN UNTUK KEAMANAN INFORMASI **KONTROL** Seperangkat kebijakan untuk keamanan informasi harus ditetapkan oleh manajemen,diterbitkan dan dikomunikasikan kepadakaryawan dan pihak luar yang terkait	KONDISI Diskominfo Kota Ambon sedang merancang system keamanan informasi dan masih dalam bentuk draft yang sedang dievaluasi bersama dengan walikota.namun ada beberapa system yang telah dimiliki oleh diskominfo kota Ambon seperti SOP Pelayanan Publik dan SOP Penanganan insiden keamanan informasi	GAP Menurut annex 5 dan control 5.1.1 ini,seharusnya kebijakan untuk kemanan informasi ini harus dibuat dan disosialisasikan kepada karyawan maupun pihak luar yang terkait	REKOMENDASI Diskominfo kota Ambon perlu merancang kebijakan keamanan informasi yang mengacu pada SMKI yang berlaku dan melakukan evaluasi serta mendapatkan persetujuan dari Walikota Ambon untuk melindungi informasi yang dimiliki	1
		SEBAB Masih melakukan evaluasi dalam bentuk draft serta belum mendapat persetujuan dari walikota Ambon	DAMPAK Upaya untuk melakukan sertifikasi sesuai dengan standart ISO yang berlaku belum bisa berjalan dengan baik karena pembentukan kebijakan dan prosedurnya belum terlalu terdefinisi		

Gambar 5. *Workpaper Gap Analysis.*

Annex	5.KEBIJAKAN KEAMANAN INFORMASI			
Kontrol Annex	5.1 ARAHAN MANAJEMEN UNTUK KEAMANAN INFORMASI			
Pertanyaan	Apakah terdapat kebijakan untuk keamanan informasi yang ditetapkan,disetujui oleh manajemen,diterbitkan dan dikomunikasikan kepada karyawan dan pihak luar yang terkait serta diriviu pada interval waktu yang terencana?			
Jumlah Kontrol Objektif	2			
Tingkat Kematangan	Kriteria	Pilihan nilai Kematangan	Nilai Kontrol Annex	Nilai Maturity Level
1	Kebijakan Keamanan Informasi belum ditetapkan/masih dalam draft perencanaan	√	1	1
2	Kebijakan Keamanan Informasi telah ditetapkan namun hanya sebagian			
3	Kebijakan Keamanan Informasi telah ditetapkan secara keseluruhan			
4	Kebijakan Keamanan Informasi telah ditetapkan secara keseluruhan dan telah dikomunikasikan			
5	Kebijakan Keamanan Informasi telah ditetapkan secara keseluruhan,telah dikomunikasikan dan diimplementasikan			
Penjelasan	Kebijakan Keamanan Informasi yang dimiliki oleh Dinas Komunikasi dan Informatika Pemerintah Kota Ambon masih dalam bentuk draft perencanaan,sehingga berdasarkan kriteria yang ditentukan maka nilai *Maturity Level* nya berada pada tingkat 1			

Gambar 6. Format *Maturity Level.*

Metodologi Penelitian

Pada penelitian ini, peneliti menggunakan jenis penelitian secara kualitataif. Oleh karena itu, peneliti akan melakukan eksplorasi terkait analisis manajemen keamanan informasi pada pemerintah Kota Ambon. Secara garis besar, penelitian ini menggunakan teknik triangulasi dalam proses pengumpulan data yaitu observasi langsung, wawancara, serta kuesioner atau *worksheet*. Selanjutnya, teknis analisis dilakukan yaitu dengan melakukan *workpaper gap analysis* dan penilaian *maturity level* atau tingkat kematangan. Hasil pengumpulan data dari objek penelitian melalui proses wawancara, observasi langsung dan kueisioner akan dimasukan ke dalam *workpaper gap analysis* yang mana analisis ini bertujuan untuk mengetahui kondisi saat ini dan membandingkan dengan standar keamanan informasi berdasarkan ISO 27002:2013. Di bawah ini merupakan contoh *workpaper gap analysis* yang digunakan dalam penelitian ini 5. Selanjutnya, setelah melakukan proses *gap analysis*, maka akan dinilai nilai *maturity level* dengan menggunakan format yang telah dibuat yang mana disesuaikan dengan standar ISO 27002:2013 dan kriteria yang diadopsi berdasarkan Permenpan No 59 Tahun 2020. Untuk format *maturity level* bisa dilihat pada gambar di bawah ini: 6

Hasil dan Pembahasan

Pembahasan dan analisis data merupakan tahap untuk melakukan apa yang telah didefinisikan pada metodologi penelitian, sehingga terdapat beberapa tahap yakni:

Gambaran Umum Objek Penelitian

Dinas Komunikasi dan Informatika Pemerintah Kota Ambon dengan Motto: "AKTUAL DAN TERPERCAYA DALAM PELAYANAN INFORMASI" merupakan dinas yang berada di bawah naungan Pemerintah Kota Ambon yang terbentuk berdasarkan "Peraturan Walikota (PERWALI) Kota Ambon Nomor 38 Tahun 2016" tentang organisasi dan tata kerja Dinas Kota Ambon.

Profil Subjek Penelitian

Data primer merupakan suatu data yang digunakan untuk proses penyelesaian penelitian ini. Oleh sebab itu pada penelitian ini, beberapa pegawai Dinas Komunikasi dan Informatika Pemerintah Kota Ambon sebagai informan yang mana bertanggung jawab dan memahami sesuai dengan penelitian yang sedang dilakukan. Secara garis besar, dua informan yang terkait yakni Kepala Bidang *E-Government* dan Kepala Bidang Teknologi Informasi Persandian dan Statistik. Analisis Keamanan Informasi

Proses Analisis

Proses analisis yang dilakukan pada Dinas Komunikasi dan Informatika Pemerintah Kota Ambon merupakan suatu tahapan penelitian yang mana mencakup serangkaian kegiatan yang dilakukan untuk proses penelitian dan pencarian data yang mana dimulai dari proses perjanjian penelitian sampai dengan proses analis data. Hasil *Assesment Evidence* (Temuan Penelitian) Hasil *assesment evidence* atau temuan penelitian ini merupakan hasil yang didapatkan ketika peneliti melakukan proses pengumpulan data. *Assesment evidence* ini bertujuan untuk memberikan bukti apa saja dokumen-dokumen yang dimiliki dinas Komunikasi dan Informatika Pemerintah Kota Ambon. Berdasarkan hasil penelitian yang dilakukan, ada beberapa temuan penelitian yang didapati dari objek penelitian seperti SOP pelayanan publik, SOP penanganan insiden, draft kebijakan keamanan informasi, surat kontrak kerja dengan pihak ketiga, dan lain-lain.

Proses Analisis Data

Setelah melalui proses pengumpulan data, maka data yang dihasilkan akan diolah dan dilakukan analisis. Berdasarkan teknik pengumpulan data yang dilakukan, peneliti selanjutnya melakukan proses pengolahan serta membuat ringkasan hasil pengolahan data, penggunaan *work paper gap analysis* dan peniliaian M*aturity Level*.

Ringkasan Data

Ringkasan Data merupakan proses meringkas hasil pengolahan data yang telah dilakukan sebelumnya dan akan disajikan dalam bentuk tabel berikut ini: 3 & 4

Work Paper GAP Analysis

Berdasarkan hasil analisis yang telah dilakukan, maka terdapat beberapa GAP pada Dinas Komunikasi dan Informatika Pemerintah Kota Ambon yang mana hasil analisis menunujukan bahwa untukk setiap *Annex* yang dilakukan penilaian, terdapat GAP yang mengakibatkan kurang stabilnya keamanan informasi pada objek penelitian.

Penilaian *Maturtiy Level*

Berdasarkan proses penelitian dan pengolahan data yang telah dilakukan oleh peneliti terhadap objek penelitian,maka telah didapatkan hasil penelitian untuk semua kontrol *Annex* ISO 27002:2013 dengan nilai *maturity level* yang berbeda-beda yang mana dalam proses penilaian ini,peneliti terlebih dahulu membuat tabel yang selanjutnya akan digunakan untuk proses penilaian sesuai dengan hasil pengolah data yang telah dilakukan. Untuk nilai *maturity level* bisa dilihat pada tabel berikut ini: 5

Pelaporan Hasil Analisis dan Rekomendasi

Setelah melakukan proses analisis data, maka tahap selanjutnya yaitu melaporkan hasil analisis yang telah dilakukan serta memberikan rekomendasi yang sesuai dengan GAP yang ada untuk meningkatkan keamanan infomasi pada Dinas Komunikasi dan Informatika Pemerintah Kota Ambon.

Laporan Hasil Analisis

Laporan hasil analisis ini merupakan ringkasan atau garis-garis besar tentang hasil analisis yang telah dilakukan sesuai dengan penelitian yang telah dilakukan.oleh sebab itu berdasarkan hasil analisis yang telah dilakukan, maka terdapat beberapa GAP pada Dinas Komunikasi dan Informatika Pemerintah Kota Ambon yang mana hasil analisis menunujukan bahwa untukk setiap *Annex* yang dilakukan penilaian, terdapat GAP yang mengakibatkan kurang stabilnya keamanan informasi pada objek penelitian. Selanjutnya, setelah melakukan proses analisis terhadap GAP yang terjadi, maka akan diketahui tingkat *maturity level* yang dimiliki oleh Dinas Komunikasi dan Informatika Pemerintah Kota Ambon dan didapatkan bahwa rata-rata nilai *maturity level* yang dimiliki berada nilai 1.84 dan berada pada level 2 (*repeteable*) yang mana pada level 2 ini didefisnikan bahwa organisasi atau instansi telah mempunyai keamanan informasi yang cukup baik tetapi belum didokumentasikan atau belum sepenuhnya berjalan sesuai dengan prosedur yang berlaku.

Selain itu, sesuai dengan hasil wawancara kembali melalui media *online*, Dinas Komunikasi dan Informatika Pemerintah Kota Ambon mempunyai nilai terget berada pada angka 3 dengan alasan bahwa kegiatan yang dilakukan masih belum optimal namun bisa untuk dilakukan secara keseluruhan sesuai denagn kriteria yang telah ditentukan sesuai dengan standar ISO 27002:2013. Selanjutnya, jika dibandingkan dengan *indeks* SPBE yang bersumber dari website resmi Dinas Komunikasi dan Informatika Pemerintah Kota Ambon yang mana dinas ini mempunyai nilai yang cukup baik yakni berada pada nilai 2.96 yang berati bahwa tingkat kematangan dinas ini berada pada level yang baik. Oleh sebab itu, berdasarkan data yang telah ditemukan, peneliti akan memberikan rekomendasi yang mana disesuaikan antara *indeks* SPBE dan juga ISO 27002:2013 agar bisa relevan atau saling berkesinambungan.

Rekomendasi

Berdasarkan hasil analisis yang telah dilakukan, terlihat bahwa setiap *Annex* yang dilakukan analisis mempunyai GAP nya masing-masing. Oleh sebab itu, adanya GAP yang terjadi berpengaruh terhadap nilai *maturity level* atau tingkat kematangan Keamanan informasi yang dimiliki oleh Dinas Komunikasi dan Informatika Pemerintah Kota Ambon yang mana berada pada level 2 (*repeteable*). Berdasarkan nilai tersebut, maka perlu diberikan Rekomendasi dengan tujuan untuk membantu objek penelitian dalam memperbaiki nilai *maturtity evel* yang dimiliki agar bisa menjaga keamanan informasi yang dimiliki. Sehingga rekomendasi itu sendiri akan diberikan terhadap semua *Annex* yang dilakukan analisi disesuaikan dengan nilai *indeks* SPBE dan juga nilai *maturity level* yang dimiliki sehingga rekomendasi yang diberikan sesuai dengan kondisi dan keadaan yang sedang terjadi. Berikut ini merupakan rekomendasi yang bisa diberikan kepada Dinas Komunikasi dan Informatika Pemerintah Kota Ambon untuk meningkatkan nilai *maturity level* ke tingkat yang lebih baik seperti mempercepat proses pembuatan draft peraturan, melakukan *riview* kebijakan keamanan informasi, mempertegas tentang pemisahan tugas dan tanggung jawab, dan lain-lain.

Table 3. Ringkasan Data

A.5	Kebijakan Keamanan Informasi	Untuk *Annex* A.5 ini Dinas Komunikasi dan Informatika Kota Ambon masih melakukan proses perancangan sistem keamanan informasi dan masih dalam bentuk draft yang akan dievaluasi dengan walikota. Namun ada beberapa sistem yang telah dimiliki oleh Dinas Komunikasi dan Informatika kota Ambon seperti SOP Pelayanan Publik dan SOP Penanganan insiden keamanan informasi.
A.6	Organisasi Keamanan Informasi	Untuk *Annex* A.6 ini Dinas Komunikasi dan Informatika Pemerintah Kota Ambon telah melakukan proses pendefinisian tanggung jawab tetapi belum secara terstruktur dikarenakan masih ada dalam proses penyusunan tupoksi dari masing-masing bidang. Dan untuk hubungan dengan pihak ketiga sudah dilakukan perjanjian melalui kontrak kerja tetapi untuk kebijakan perangkat bergerak dan teleworking belum dijalankan karena masih ada dalam proses perancangan draft peraturannya.
A.7	Keamanan Sumber Daya Manusia	Untuk *Annex* A.7 ini Dinas Komunikasi dan Informatika pemerintah kota Ambon telah melakukan proses penyaringan terhadap calon pegawai secara umum sesuai dengan regulasi tetapi untuk bidang keamanan informasi sendiri belum ada prosedur khusus. Serta telah melakukan perjanjian dengan pihak ketiga terkait dengan syarat dan ketentuan kepegawaian, tanggung jawab manajemen tetapi dengan pegawai belum dilaksanakan.serta telah membuat proses pelatihan kepada pegawai untuk meningkatkan kemampuan yang dimiliki serta telah melakukan proses pendisiplinan dan penghentian atau perubahan tanggung jawab.
A.8	Manajemen Aset	Untuk *Annex* A.8 ini Dinas Komunikasi dan Informatika Pemerintah Kota Ambon telah melakukan beberapa hal yang terkait yakni telah melakukan proses tanggung jawab terhadap aset yang mana setiap aset telah diinventaris oleh pihak yang telah diberikan tugas dan tanggung jawab, serta telah melakukan proses klasifikasi informasi dan pelabelan informasi, serta telah melakukan proses penanganan media seperti proses manajemen media yang dapat dipindahkan yang mana menggunakan beberapa media seperti hardisk, flashdisk, google drive dan lain-lain.
A.9	Kendali Akses	Untuk *Annex* A.9 ini Dinas Komunikasi dan Informatika Pemerintah Kota Ambon telah melakukan proses kendali akses yang mana telah dilakukan proses kebijakan untuk pengendalian akses dan hanya personil tertentu yang bisa mengakses informasi yang bersifat rahasia. Namun hak ases yang dikendalikan hanya untuk sistem yang berisi informasi, namun untuk proses hak akses seperti ke ruang server dan masuk ruangan belum dilakukan secara otomatis atau masih dilakukan secara manual dengan menggunakan kunci ruangan.
A.10	Kriptografi	Untuk *Annex* A.10 ini Dinas Komunikasi dan Informatika telah melakukan proses kriptografi melalui penggunaan sertifikat elektronik,tetapi untuk manajamen kata kunci hanya menggunakan *password* saja.

Kesimpulan

Setelah melakukan semua alur penelitian yang telah didefinisikan sebelumnya, maka tahap selanjutnya yaitu tahap kesimpulan yang merupakan tahap terakhir dari penelitian yang dilakukan. Berdasarkan rumusan masalah dan tujuan penelitian serta hasil pengolahan dan analisis data, maka kesimpulan yang didapatkan dari penelitian yang telah dilakukan yaitu sebagai berikut:

1. Terdapat beberapa hasil penelitian atau temuan seperti file draft kebijakan keamanan informasi, SOP Penangangan insiden, file persyaratan penerimaan pegawai, surat pengendalian hak akses dari kepala dinas, surat perjanjian kontrak kerja dengan pihak ketiga, serta draft perencaan lainnya.
2. Berdasarkan hasil pengolahan dan analisis data yang telah dilakukan, maka ditemukan bahwa Dinas Komunikasi dan Informatika Pemerintah Kota Ambon sebagai objek penelitian mempunyai GAP untuk semua kontrol *Annex* ISO 27002:2013 yang dijadikan sebagai ruang lingkup penelitian. Ini berarti bahwa kondisi keamanan informasi yang dimiliki oleh objek penelitian sebagian besar belum sesuai dengan standar yang telah ditentukan. Dari 114 kontrol objektif yang ada, Dinas Komunikasi dan Informatika Pemerintah Kota Ambon hanya menjalankan beberapa kontrol dan oleh sebab itu sehingga ditemukan GAP, maka nilai rata-rata *maturity level* atau tingkat kematangan yang dimiliki oleh Dinas Komunikasi dan Informatika Pemerintah Kota Ambon berada pada nilai 1.84 dengan level kematangan pada kategori *repeteable* yang berarti bahwa keamanan informasi yang dimiliki oleh objek penelitian tergolong rendah dan harus dilakukan perbaikan atau rekomendasi untuk memperbaiki serta meningkatkan keamanan informasi itu sendiri.
3. Karena mempunyai GAP yang dimiliki oleh setiap kontrol *Annex* dan nilai *maturity level* yang rendah, maka diperlukan rekomendasi yang bisa membantu objek penelitian untuk memperbaiki

Table 4. Ringkasan Data

Annex	**Nama *Annex***	**Ringkasan**
A.11	Keamanan Fisik dan Lingkungan	Untuk *Annex* A.11 ini Dinas Komunikasi dan Informatika telah melakukankeamanan fisik dan lingkungan tetapi belum secara terstruktur. Pada ruang server, bisa dimasuki oleh semua pegawai hanya dengan menulis keperluanpada papan tulis yang telah disediakan di depan ruang server tersebut. Untuk pengamanan ruangan juga hanya masih menggunakan kunci dan beberapa cctv,dan untuk area bingkar muat belum dilaksanakan karena masih dalam proses penganggaran tahun untuk tahun depan. Dan untuk bagian hal teknis seperti kabel, Dinas Komunikasi dan Informatika kota Ambon melakukan karena masih dalam proses penganggaran atau masih dalam proses perancangan.
A.12	Keamanan Operasi	Untuk *Annex* A.12 ini sebagian besar Dinas Komunikasi dan Informatika Kota Ambon belum melakukan proses terhadap keamanan operasi dikarenakan masih dianggarkan dan masih dalam proses pengembangan. Namun ada beberapa yang sudah dilakukan seperti pencadangan dan pemantauan terhadap informasi log yang ada
A.13	Keamanan Komunikasi	Untuk *Annex* A.13 ini Dinas Komunikasi dan Informatika Kota Ambontelah melakukan proses kendali jaringan dan perjanjian kerahasiaan dengan pihak ketiga tetapi untuk proses pemindahan informasi masih belumdilaksanakan karena masih dalam proses perencanaan.
A.14	Akuisisi, pengembangandan Perawatan sistem	Untuk *Annex* A.14 ini Dinas Komunikasi dan Informatika Kota Ambonsecara umum belum menerapkan dengan alasan bahwa masih dalam tahap pengembangan dan sedang dianggarkan tahun depan.
A.15	Hubungan Pemasok	Untuk *Annex* A.15 ini Dinas Komunikasi dan Informatika Kota Ambon secara umum belum menerapkan dengan alasan bahwa masih dalam tahap pengembangan dan sedang dianggarkan tahun depan.
A.16	Manajemen Insiden Keamanan Informasi	Untuk *Annex* A.16 ini Dinas Komunikasi dan Informatika Kota Ambon telah melakukan proses tanggung jawab ketika terjadi manajemen keamanan informasi melalui personil yang telah dilakukan tanggung jawab tetapi belum efisien karena kurangnya pemantauan secara langsung oleh pihak yang berwenang
A.17	Keamanan Informasi dari manajemen keberlangsungan bisnis	Untuk *Annex* A.17 ini Dinas Komunikasi dan Informatika Kota Ambon secara umum belum menerapkan dengan alasan bahwa masih dalam tahap pengembangan dan sedang dianggarkan tahun depan.
A.18	Kesesuaian	Untuk *Annex* A.18 ini Dinas Komunikasi dan Informatika Kota Ambon secara umum belum menerapkan dengan alasan bahwa masih dalam tahap pengembangan dan sedang dianggarkan tahun depan.

serta meningkatkan manajemen keamanan informasi yang dimiliki. Rekomendasi diberikan untuk 14 Kontrol *Annex* yang ada sesuai dengan definisi dari kontrol itu sendiri. Ada beberapa rekomendasi yang diberikan seperti melakukan *riview* kebijakan keamanan informasi minimal 3 bulan sekali, mempercepat penyusunan tupoksi masing-masing bidang, melakukan pergantian *password* secara berkala, melakukan kunci ruangan otomatis, melakukan *riview* terhadap hak akses yang telah diberikan, menjaga hubungan baik dengan pihak yang berwenang, serta melakukan pengawasan terhadap personil yang bertanggung jawab tentang keamanan informasi.

Daftar Pustaka

1. Zuhroh NF. TA: Perencanaan Sistem Manajemen Keamanan Informasi Pada Information Capital Readiness PT PJB UP Gresik. Institut Bisnis dan Informatika Stikom Surabaya; 2017.

Table 5. Penilaian *Maturtiy Level*

Annex	**Nama *Annex***	**Nilai *Maturity Level***	**Keterangan**
A.5	Kebijakan Keamanan Informasi	1	*Initial* (1)
A.6	Organisasi Keamanan Informasi	1.5	*Initial* (1)
A.7	Keamanan Sumber Daya Manusia	2.88	*Defined* (3)
A.8	Manajemen Aset	2.66	*Defined* (3)
A.9	Kendali Akses	1.95	*Repeteable* (2)
A.10	Kriptografi	2.50	*Repeteable* (2)
A.11	Keamanan Fisik dan Lingkungan	1.55	*Repeteable* (2)
A.12	Keamanan Operasi	2.42	*Repeteable* (2)
A.13	Keamanan Komunikasi	2.05	*Repeteable* (2)
A.14	Akuisisi, pengembangan dan Perawatan sistem	1.06	*Initial* (1)
A.15	Hubungan Pemasok	1	*Initial* (1)
A.16	Manajemen Insiden Keamanan Informasi	2	*Repeteable* (2)
A.17	Aspek Keamanan Informasi dari manajemen keberlangsungan bisnis	1	*Initial* (1)
A.18	Kesesuaian	2.20	*Repeteable* (2)
Rata-Rata		1,84	*Repeteable* (2)

2. Ikhsan M, Suwawi DDJ, et al. Audit keamanan sistem informasi akademik Sekolah Tinggi Farmasi Bandung berbasis risiko dengan menggunakan standar ISO 27001. eProceedings of Engineering. 2016;3(3).
3. Bernard P. Foundations of ITIL® 2011 Edition. Van Haren; 1970.
4. Kurniawan E, et al. Analisis tingkat keamanan sistem informasi akademik berdasarkan standard ISO/IEC 27002: 2013 menggunakan SSE-CMM. Universitas Islam Indonesia; 2018.
5. Carolina I. Analisa Penilaian Maturity Level Tata Kelola Ti Berdasarkan Domain DS Dan ME Menggunakan Cobit 4.1. SNIT 2015. 2015;1(1):190-5.
6. Supriyatna A. Analisis Tingkat Keamanan Sistem Informasi Akademik dengan Mengkombinasikan Standar Bs-7799 dengan SSE-CMM. In: Prosiding Seminar Nasional Aplikasi Sains & Teknologi (SNAST). 182; 2014. .
7. Afandi H, Darmawan A. Audit Kemanan Informasi Menggunakan Iso 27002 Pada Data Center Pt. Gigipatra Multimedia. Jurnal Teknologi Informasi Magister. 2015;1(02):175-91.
8. Wicaksono BB. Evaluasi Keamanan Informasi Berdasarkan ISO/IEC 27002: 2013 Information Security Management System: Studi Kasus Perusahaan XYZ. Program Studi Sistem Informasi FTI-UKSW; 2018.
9. Pajar IR. Analisis Tingkat Keamanan Aplikasi SIMAK Menggunakan Standard ISO/IEC 27002:2013 (Studi Kasus: UPTTIK Universitas Siliwangi). Jurnal Serambi Engineering. 2021 mar;6(2). Available from: https://doi.org/10.32672%2Fjse.v6i2.2879.