IMPLEMENTASI PENGELOLAAN PERSANDIAN DALAM RANGKA KEAMANAN INFORMASI DI DINAS KOMUNIKASI DAN INFORMATIKA KOTA MADIUN

Archan Rismananda
NPP. 30.0778
Asdaf Kota Madiun, Provinsi Jawa Timur
Program Studi Teknologi Rekayasa Informasi Pemerintahan
Email: archanrismananda482@gmail.com

Pembimbing Skripsi: Dedhy Guntoro., SE, MM

ABSTRACT (in english)
(sesuaikan dengan model abstrak terstruktur berikut ini mulai dari Problem Statement s.d. Keyword)

Problem Statement/Background (GAP): (The basis for the creation of this research is data leakage in the government environment, one of the leaked information security systems is guarded by using encryption. Encryption is an activity of securing data/information carried out using crypto principles, theory, art and science, as well as other supporting knowledge, in a systematic, methodical and consistent manner, and bound to encryption. Encryption is one of those mandatory things that are not related to any underlying services. **Purpose:** The purpose of this study is to collect information and describe how the implementation of encryption in maintaining information security, as well as assess the readiness of the Office of Communication and Informatics in implementing information security using Indeks KAMl 4.2 in the Office of Communication and Informatics, City of Madiun. **Method:** In this study, Edward III's Implementation theory was used and combined with the Indeks KAMI 4.2 while data collection was carried out through qualitative research using inductive descriptive methods which included interviews, observation, and documentation approaches. The data analysis approach uses data reduction, data presentation, and data verification. **Result:** Using Edward III's implementation theory, it was found that in the field the situation in the management of cryptography has been carried out well, this is shown from the point of view of communication that has been carried out well, existing resources have been optimal, dispositions have been carried out well, and appointments of bureaucrats that have been appropriate. Also supported in the assessment using the Indeks KAMI 4.2, a high score was obtained. **Conclusion:** Based on the results of research that has been carried out by researchers, it is found that the management of encryption has followed the existing SOPs and standards. This can be seen from the ISO 27001:2013 certificate that has been owned and the results of the Indeks KAMI, which is 624, which is included in the level of readiness for encryption management, which has a "Good" level.
Keywords: Encryption; Implementation; Information; Security

ABSTRAK

Permasalahan/Latar Belakang (GAP): Dasar terciptanya penelitian ini adalah kebocoran data di lingkungan pemerintah, salah satu sistem keamanan informasi yang mengalami kebocoran dijaga dengan menggunakan persandian. Persandian adalah kegiatan pengamanan data/informasi yang dilakukan dengan menggunakan prinsip, teori, seni, dan ilmu kripto, serta ilmu pendukung lainnya,

secara sistematis, metodis, dan konsisten, serta terikat pada persandian. Persandian adalah salah satu hal wajib yang tidak terkait dengan layanan mendasar. **Tujuan:** Tujuan dari penelitian ini adalah untuk mengumpulkan informasi dan mendeskripsikan bagaimana implementtasi persandian dalam menjaga keamanan informasi, serta menilai kesiapan Dinas Komunikasi dan Informatika dalam mengimplementasikan keamanan informasi dengan menggunakan Indeks KAMl 4.2 di Dinas Komunikasi dan Informatika Kota Madiun. **Metode:** Dalam penelitian ini menggunakan teori Implementasi Edward III serta dipadukan dengan menggunakan Indeks KAMI 4.2 sedangkan pengumpulan data dilakukan melalui penelitian kualitatif dengan metode deskriptif induktif yang meliputi pendekatan wawancara, observasi, dan dokumentasi. Pendekatan analisis data menggunakan reduksi data, penyajian data, dan verifikasi data. **Hasil/Temuan:** menggunakan teori implementasi Edward III diperoleh situasi dilapangan yang dalam pengelolaan persandian telah dilakukan dengan baik hal ini ditunjukkan dari mulai segi komunikasi yang telah dijalankan dengan baik, sumber daya yang ada telah optimal, disposisi yang telah dilakukan dengan baik, dan pengangkatan birokrat yang sudah tepat. Ditunjang juga dalam penilaian menggunakan Indeks KAMI 4.2 diperoleh nilai yang tinggi. **Kesimpulan:** Berdasarkan hasil penelitian yang telah dilakukan oleh peneliti maka diperoleh bahwa dalam pengelolaan persandian telah mengikuti SOP dan standar yang ada. Hal ini dapat dilihat dari sertifikat ISO 27001:2013 yang telah dimiliki serta hasil Indeks KAMI yaitu 624 yang masuk dalam tingkat kesiapan pengelolaan persandian memiliki tingkat yang “Baik”.
Kata kunci: Implementasi; Informasi; Keamanan; Persandian

I. PENDAHULUAN

1.1. Latar Belakang

Kebutuhan terhadap teknologi saat ini sangatlah penting perananya dalam kehidupan manusia hal ini ditandai dengan semakin berkembangnya teknologi yang ada guna membantu mempermudah aktivitas maupun pekerjaan manusia. Setiawan & Mustofa mengemukakan bahwa Pemanfaatan teknologi komunikasi dan informasi dalam proses pemerintahan (e-government) akan meningkatkan efisiensi, efektivitas, transparansi (Setiawan & Mustofa, 2013). Kemajuan teknologi informasi (TI) berkembang pesat. Akibatnya, seluruh organisasi atau perusahaan harus terus-menerus mengubah dan menggabungkan peningkatan TI. Ada informasi yang diolah dan disimpan dalam perkembangan teknologi yang semakin cepat. Sudjiman mendefinisikan Informasi adalah data yang dapat digunakan dalam proses pengambilan keputusan (Sudjiman & Sudjiman, 2018). Maka dari itu, Untuk menjaga keamanan informasi, perlu dilakukan upaya untuk menjamin keamanan semua perangkat pendukung, jaringan, dan fasilitas lain yang secara langsung atau tidak langsung terkait dengan pemrosesan informasi tersebut.

Hal utama yang berbpengaruh pada Teknologi Informasi ialah Keamanan Informasi. Keamanan Informasi adalah unsur penting yang harus diperhatikan dalam memanajemen Teknologi informasi. Dalam hal keamanan informasi perlu dilakukan pengukuran kekuatan dalam penerapan keamanan informasi (Disterer, 2013). Pada Keamanan Informasi perlu adanya evaluasi dan inovasi karena perkembangannya yang begitu cepat pada era saat ini.

Keamanan informasi ini sangat penting, terutama dalam praktek pemerintah baik di tingkat pusat maupun daerah. Hal ini harus dilakukan guna melindungi informasi dan data negara yang penting. Di era saat ini maraknya kejahatan siber yang sering terjadi di Indonesia perlu dilakukan respon atau tindakan pencegahan yang cepat dan tepat.

Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN), pada sepanjang tahun 2021 telah terjadi sebanyak 1.637.973.022 serangan siber yang terjadi di Indonesia. Dari keseluruhan serangan ini sebanyak 44,62% didominasi dari *MyloBot Botnet*. Yang mana *MyloBot Botnet* merupakan salah satu media yang digunakan untuk mencuri data melalui jaringan komputer.

Sebagai contohnya adalah kebocoran data yang terjadi pada Badan Penyelenggaraan Jaminan Sosial (BPJS) yang mana sebanyak 279 juta data peserta BPJS telah bocor. Data yang bocor ini dapat disalahgunakan oleh pihak yang tidak bertanggung jawab, yang mengakibatkan kerugian yang signifikan bagi pemilik data.

Kasus lain selain Kasus BPJS, saat ini sedang hangat menjadi perbincangan mengenai kebocoran data pemerintah yang dilakukan oleh *hacker* dengan nama Bjorka. Dalam kasusu ini data pemerintah yang diklaim bocor adalah data pelanggan indihome, data KPU, data *SIM Card*, dan lain sebagainya. Hal ini menunjukkan bahwa perlu adanya pembenahan dalam pengamanan informasi oleh pemerintah.

Berjalannya waktu kewaktu serangan siber terus berumbuh dan meningkat hal ini sejalan dengan meningkatnya pengguna media informasi secara digital. Semakin banyak pengguna media digital maka semakin besar juga resiko serangan siber yang terjadi. Maka dari itu dengan perkembangan *e-government* di Indonesia pemerintah melalui instruksi presiden nomor 3 tahun 2003 tentang kebijakan dan strategi nasional pengembangan *E-Government* maka pemerintah telah Menyusun beberapa Langkah strategis untuk menunjang dan mendukung dalam pengembangan *e-government* salah satunya adalah mengenai keamanan informasi. Hal ini juga didukung dengan Peraturan Menteri Komunikasi dan Informatika Nomor 4 tahun 2016 tentang Sistem Manajemen Pengamanan Informasi. Dalam hal ini untuk menilai bagaimana pengelolaan keamanan informasi maka disesuaikan dengan ISO 27001 yang juga diaplikasikan paka Indeks KAMI (Indeks Keamanan Informasi. Sebagai acuan dalam manila tingkat kesiapan dalam penerapan keamanan informasi.

1.2. Kesenjangan Masalah yang Diambil (GAP Penelitian)

Berjalannya waktu kewaktu serangan siber terus berumbuh dan meningkat hal ini sejalan dengan meningkatnya pengguna media informasi secara digital. Semakin banyak pengguna media digital maka semakin besar juga resiko serangan siber yang terjadi. Terutama pada tata Kelola Pemerintah saat ini yang telah berubah menjadi serba digital, hal ini besar kemungkinan menimbulkan suatu hambatan baru dalam praktek penyelenggaraanya berkaitan dengan keamanan informasi. Maka dari utu diperlukan upaya yang signifikan dalam pengamanan informasi yang dibuat dalam standar yang baik sehingga dapat meminimalisir terjadinya kebocoran data ataupun kerugian yang menimpa masyarakat maupun pemerintah. Berdasarkan hal-hal tersebut diatas maka sejauhmana pengelolaan persandian yang telah dilakukan pemerintah khususnya Kota Madiun yang ini menjadi menarik untuk dikaji dan diteliti berdasar pada fakta dan kondisi asli dilapangan untuk penulis teliti lebih dalam mengenai implementasinya dalam pengelolaan persandian untuk menjaga keamanan informasi serta mengetauhi seberapa tingkat kesiapan yang telah dilakukan.

1.3. Penelitian Terdahulu

Penelitian ini terinspirasi oleh beberapa penelitian terdahulu, beberapa diantaranya yaitu penelitian dari Fairzah A Basyarahil tahun 2017 tentang "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berbasis ISO/IEC 27001:2013 di Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya" Evaluasi terhadap 5 zona yang terdapat dalam Indeks Kami adalah 249 dari total 645 dan ditempatkan pada level I-II dimana level ini berada pada tahap awal implementasi keamanan data dan implementasi kerangka kerja dalam keamanan data. Tingkatan pada tiap area dapat diketahui bahwa Zona Tata Kelola Keamanan Data terletak pada tingkatan I+, zona Pengelolaan Resiko Keamanan Data pada tingkatan I, zona Kerangka kerja Pengelolaan Keamanan Data pada tingkatan I+, zona Pengelolaan Peninggalan Data pada tingkatan I+, serta zona Teknologi dan Keamanan Data pada tingkatan II (Basyarahil, 2017). Penelitian selanjutnya, penelitian dari Edo Rizky Pratama tahun 2018 tentang "Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi dengan Menggunakan Indeks KAMI dan ISO 27001 (Studi

Kasus KOMINFO Provinsi Jawa Timur)" dicapai jika kematangan dan kelengkapan keamanan informasi KOMINFO masih belum memadai. Ketidaklengkapan dan kematangan keamanan informasi ini disebabkan karena KOMINFO belum mengimplementasikan seluruh komponen kebutuhan keamanan informasi yang masih dalam tahap perencanaan. Diagram batang yang ada saat ini, yang berwarna merah dengan skor total 245, menunjukkan tingkat kelengkapan yang rendah, yang dapat dibaca sebagai indikasi bahwa keamanan informasi di Dinas Komunikasi dan Informatika Provinsi Jawa Timur belum layak sehingga perlu ditingkatkan. Sedangkan tingkat kematangan setiap tingkat keamanan informasi adalah I+ (Pratama, 2018). Penelitian selanjutnya, penelitian dari Muhammad Ramadhan Slamet tahun 2019 berjudul "Penilaian Pegamanan Teknologi Pada Sistem Pembelajaran Elektronik Menggunakan Indeks Keamanan Informasi Di Politeknik Negeri Batam" diperoleh jika dalam penelitian ini yang berlokasi di Politeknik Negeri Batam menggunakan indeks KAMI untuk menentukan tingkat kematangan keamanan informasi (Slamet et al., 2019). Penelitian selanjutnya, penelitian yang dilakukan oleh Mohamat Iqbal pada tahun 2021 tentang " Evaluasi Keamanan Sistem Informasi RSUD Arifin Achmad Pekanbaru Menggunakan ISO 27001" sebagai alat bantu untuk mengukur, menganalisa serta mengevaluasi tingkat dari pengelolaan keamanan informsai pada RSUD Arifin Achmad Pekanbaru yang sesuai dengan kriteria ISO 27001 maka digunakanlah Indeks Keamanan Informasi (Indeks KAMI) (Iqbal, 2021). Penelitian selanjutnya oleh Shella Indah Dwi Octaviani berjudul "EvaIuasi Kesiapan Kerangka Kerja Keamanan lnformasi Pada Dinas Komunikasi Dan lnformatika Kota Batu Dengan Menggunakan lndeks KAMl" bahwa Dinas Komunikasi dan Informatika Kota Batu berada padapkategori rendah dengan skor 203 untuk tingkat kelengkapan, karena belum menerapkan semua syarat keamanan informasipatau masih dalam tahap perencanaan. pSedangkan untuk tingkat kematangan setiap areapkeamanan informasipberada padapLevel I sampai Level I+ (Octaviani, 2019).

1.4. Pernyataan Kebaruan Ilmiah

Penulis melakukan penelitian yang berbeda dan belum dilakukan oleh penelitian terdahulu, dimana konteks penelitian yang dilakukan yakni Perbedaan pada penyusunan yang dilakukan peneliti saat ini adalah peneliti mengkombinasikan model Implementasi dari Edward III dengan Indek KAMI Versi 4.2 yang mana merupakan versi terbaru. Model Implementasi Edward III dipakai oleh penulis untuk mengetahui implementasi pengelolaan persandian yang ada pada Dinas Komunikasi dan Informatika disamping memakai Indeks KAMI 4.2 untuk mengukur tingkat dari penerapan keamanan informasi yang ada.

1.5. Tujuan.

Penelitian ini bertujuan untuk mengetahui bagaimana implementasi pengelolaan persandian dan juga tingkat kesiapan dalam penerapan keamanan informasi di Dinas Komunikasi dan Informatika Kota Madiun.

II. METODE

Penelitian ini menggunakan jenis penelitian kualitatif deskriptif. Menurut Creswell Metode kualitatif ini mengandalkan metode dengan cara mendeskripsikan serta mengeksplorasi dan juga menggali dari narasumber berkaitan dengan topik yang diteliti(Creswell, 2014). Dengan kata lain, hasil wawancara diambil oleh peneliti kemudian diukur menggunakan instrument sehingga menghasilkan suatu Analisa berupa statistik dan kemudian akan dideskripsikan sedemikian rupa. Dalam penelitian ini menggunakan beberapa teknik pengumpulan data sebagai berikut

1. Wawancara

Wawancara yang dilakukan pada penelitian ini adalah jenis wawancara semi terstruktur. merupakan wawancara yang dilakukan dengan cara memberikan pertanyaan secara bebas akan tetapi masih tetap berada pada pedoman wawancara yang sebelumnya telah dibuat. Cara ini digunakan penulis guna memperoleh informasi dan data yang diperlukan menegenai pengelolaan persandian di Dinas Komunikasi dan Informatika Kota Madiun.

2. Observasi

Observasi adalah kegiatan manusia yang melibatkan penggunaan panca indera, dengan mata berfungsi sebagai perangkat utama dalam sistem, di samping indera lain seperti mulut, kulit, penciuman, dan pendengaran. Pendekatan ini mengharuskan penulis untuk mengamati topik penelitian secara langsung maupun tidak langsung dengan menggunakan alat bantu berupa petunjuk penelitian berupa lembar observasi atau lainnya.

Pada penelitian ini Observasi dilakukan pada Dinas Komunikasi dan Informatika dengan cara menulis segala Informasi yang didapatkan dan diperlukan untuk penulisan penelitian.

3. Dokumentasi

Dokumentasi ini, menurut para ahli, merupakan sarana pengumpulan data yang tidak langsung ditentukan pada subjek penelitian. Dokumen dapat dalam berbagai bentuk, termasuk jurnal, surat pribadi, catatan dari berbagai situasi profesional, dan materi lainnya yang telah dilengkapi.

III. HASIL DAN PEMBAHASAN

3.1. Implementasi Pengelolaan Persandian Dalam Rangka Keamanan Informasi di Dinas Komunikasi dan Informatika Kota Madiun

Penulis melakukan penelitian menggunakan teori implementasi Edward III dan Indeks KAMI 4.2 dalam melakukan penelitian mengenai pengelolaan Persandian di Dinas Komunikasi dan Informatika Kota Madiun. Terdapat 44 dimensi pada teori implementasi ini.

1. Komunikasi

Komunikasi merupakan proses penyampaian informasi dari komunikator kepada komunikan. Sementara itu, komunikasi kebijakan berarti proses penyampaian informasi kebijakan dan pembuat kebijakan kepada pelaksana kebijakan. Komunikasi yang dilaksanakan dalam implementasi pengelolaan persandian dalam rangka keamanan informasi sudah dilakukan dengan baik. Hal ini terbukt berdasarkan hasil wawancara yang dilakukan penulis yang mana jawaban yang diberikan menggambarkan bahwa proses komunikasi sudah berjalan dengan baik. Komunikasi mengenai pengelolaan persandian dalam rangka keamanan informasi sangat diperlukan sehingga seluruh lini pada instansi dapat memahami tupoksinya masing-masing dalam proses pengelolaan keamanan informasi tersebut.

Transmisi (penyampaian informasi) adalah faktor pertama dalam indikator komunikasi, sebelum pegawai atau staf pelaksana melakukan pekerjaan, harusnya mereka mengetahui lebih dulu apa yang akan dilakukan tersebut telah sesuai perintah atau instruksi pembuat kebijakan atau program. Hal itu harus menjadi perhatian khusus karena apabila terjadi distorsi dari proses transmisi (penyampaian informasi) maka akan mengakibatkan program yang diluncurkan oleh instansi akan disampaikan berlainan kepada pelaksana. transmisi menghendaki agar informasi disampaikan tidak hanya pada unsur pimpinan organisasi tapi juga sampai pada pelaksana ataupun eksekutor dari program tersebut,

seperti pada pengelolaan keamanan informasi ini harus sampai pada lini paling bawah yaitu hingga staff dalam seksi pengelolaan keamanan inforrmasi dan persandian tersebut.
Petunjuk pelaksanaan dalam proses implementasi pengelolaan keamanan informasi bermulai dari penyampaian yang jelas dari Pusat yaitu BSSN selaku yang membuat standar dalam pengelolaan keamanan informasi yang didasarkan pada standar internasional yang kemudian secara berjenjang di informasikan kepada Dinas Komunikasi dan Informatika Kota Madiun selaku pelaksana yang kemudian dilanjutkan dengan koordinasi kepada setiap bagian sesuai tugas pokok dan fungsi pada satuan kerja di dinas komunikasi dan informatika secara jelas menerima informasi mengenai mekanisme pengelolaan keamanan informasi. Dalam pelaksanaannya sesuai dengan pernyataan diatas bahwa Dinas Komunikasi dan Informatika Kota Madiun dalam pelaksanaan pengelolaan persandian telah berpedoman sesuai dengan ISO 27001:2013 yang mana menjadi dasar atau standar dalam melaksanakan pengelolaan keamanan informasi. Serta koordinasi yang dilakukan dalam pengelolaan keamanan informasi dengan BSSN selaku badan yang bertugas dalam pengamanan informasi secara nasional.
Pelaksanaan pengelolaan persandian dalam rangka keamanan informasi dilaksanakan secara berkala baik secara fisik maupun non-fisik. Dengan pembagian pengamanan tersebut secara fisik maupun non fisik sehingga dapat dikelompokkan seefektif mungkin yang membuat pegawai atau staff pada pengelolaan keamanan informasi bekerja secara maksimal sesuai dengan tugas dan tanggung jawab yang ada.

2. Sumber Daya

Berkaitan dengan implementasi pengelolaan persandian dengan sumber daya manusia atau pegawai sebagai pelaksana dalam proses pengamanan informasi sangatlah penting, hal ini dimana pegawai sebagai pelaksana merupakan penentu keberhasilan dalam pengelolaan keamanan informasi. Jika sumber daya manusia masih kurang kompeten atau kurang memadai maka akan sangat berpengaruh pada eksekusi pengelolaan keamanan informasi sehingga tidak bisa diimplementasikan dengan baik.
Sumber Daya Manusia merupakan pemeran utama dalam terwujudnya tujuan suatu kebijakan Sumber daya manusia yang bermutu dan professional merupakan kunci utama dalam meningkatkan kualitas pelayanan. Maka dari itu untuk dapat mewujudkan pengelolaan keamanan informasi yang baik sumber daya manusia berperan penting sebagai makhluk yang mampu mengelola dirinya dan juga seluruh potensi yang ada didalam dirinya sehingga dapat mencapai potensi maksimalnya. Pada implementasi pengelolaan persandian masing-masing orang mempunyai tugas dan fungsinya masing-masing. Dalam menjalankan tugas dan fungsinya setiap lini telah melakukan secara baik sesuai pembagiannya.
Anggaran berfungsi sebagai perencanaan dan pengendalian kegiatan. Pendanaan pada suatu organisasi atau program berfungsi sebagai sumber untuk membantu dalam pemenuhan kebutuhan program. Pendanaan atau anggaran dalam pelaksanaan kegiatan pengelolaan persandian berasal dari Anggaran Pendapatan Belanja Daerah (APBD). Berdasarkan hasil dokumentasi yang dilakukan diketahui bahwa anggaran untuk Seksi Pengelolaan Keamanan Informasi dan Persandian adalah sebesar Rp. 350.000.000.
Kewenangan dalam pengelolaan keamanan sudah menjadi tugas dan tanggungjawab dari setiap lini yang terlibat dalam pengamanan informasi. Dalam wewenangnya semua berdasarkan pada ISO 27001:2013 yang mana telah dijelasakan. dapat ditarik suatu kesimpulan jika wewenang yang diberikan telah berjalan dengan baik yang mana dalam proses pengelolaan keamanan informasi didasarkan pada SOP dari standar ISO 27001:2013 dimana setiap pegawai melaksanakan tugas pokok dan fungsinya masing-masing. Hal ini dapat dilihat dari eksekusi dalam pengamanan informasi baik dari segi sarana dan prasarana serta prosedurnya yang berpedoman pada SOP.

Fasilitas merupakan sumber daya yang mendukung aparatur dalam menjalankan operasional baik dari sarana maupun prasarana. Pelayanan yang ditunjang dengan peralatan yang memadai dapat menjadi modal dalam mewujudkan program yang telah ditetapkan dengan baik.
terkait sarana dan prasarana menunjukkan jika Dinas Komunikasi dan Informatika Kota Madiun dalam hal sarana sudah maksimal dalam pengelolaan keamanan informasi. Hal ini dapat dilihat dari peralatan ataupun perangkat yang ada dalam menunjang keamanan informasi mulai dari *antivirus*, *firewall*, hingga scanning untuk mendeteksi kerentanan *hacking*. Kemudian terdapat juga perangkat keras seperti server, jaringan, dan juga system penyimpanan. Serta perangkat lunak dalam pengelolaan keamanan informasi seperti system operasi, perangkat lunak manajemen keamanan.
Sedangkan prasarana dalam pengelolaan keamanan informasi seperti kebijakan dalam keamanan informasi yang mencakup kebijakan akses, kebijakan password, serta kebijakan penghapusan data. Kemudian prosedur keamanan informasi yang mencakup prosedur dalam pengelolaan aksea, pengelolaan insiden, serta pengelolaan risiko keamaan.

3. Disposisi

Disposisi atau sikap pelaksana kebijakan adalah faktor penting dalam pendekatan mengenai pelaksanaan suatu kebijakan publik. Jika pelaksanaan suatu kebijakan ingin efektif, maka para pelaksana kebijakan tidak hanya harus mengetahui apa yang apa dilakukan tetapi juga harus memiliki kemampuan untuk melaksanakannya, sehingga dalam praktiknya tidak terjadi bias.
Pengangkatan birokrat adalah proses penerimaan seseorang sebagai pegawai negeri atau karyawan pada lembaga pemerintahan atau badan usaha milik negara. Pengangkatan birokrat dilakukan berdasarkan kebutuhan organisasi, sehingga jumlah dan jenis jabatan yang dibutuhkan juga dapat berbeda-beda pada setiap instansi atau perusahaan.
Insentif merupakan suatu penghargaan dalam bentuk material maupun non material yang diberikan oleh pihak pimpinan kepada pegawai dengan tujuan agar mereka bekerja dengan motivasi yang tinggi dan berprestasi dalam mencapai tujuan-tujuan terhadap prestasi kerja dan kontribusi pegawai.

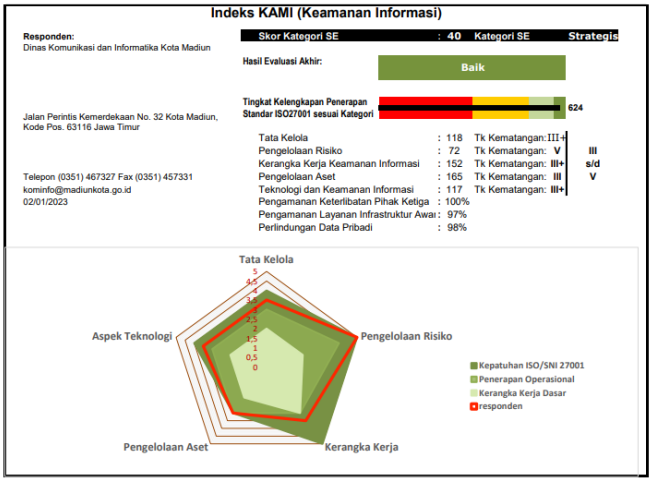
4. Struktur Organisasi

Struktur birokrasi atau organisasi merupakan wadah bagi sekelompok orang yang bekerja sama untuk mencapai tujuan yang telah ditentukan. Struktur birokrasi mempunyai peran penting yang berpengaruh dalam kesuksesan implementasi suatu program dan kebijakan, meskipun sumber-sumber dalam melaksanakan suatu program tersebut tersedia atau staf pelaksana program tersebut telah mengetahui apa yang harus dilakukan Program yang begitu kompleks meminta adanya kerjasama yang baik antar pegawai sebagai pelaksana.
SOP merupakan pedoman serta acuan tertulis bagi sta pelaksana dalam melaksanakan pekerjaannya. SOP juga merupakan hal yang sangat diperlukan dalam pelaksanaan pengelolaan persandian dalam rangka keamanan informasi yang baik. Sehingga kejelasan SOP dalam pengelolaan persandian ini menjadi penentu dalam keberhasilan pengelolaan. SOP ini sangat diperlukan dengan tujuan agar implementasi pengelolaan tidak keluar jalur serta tepat sasaran sesuai dengan tujuannya. Setidaknya ada 38 SOP yang harus dijalankan oleh pengelola persandian jika merujuk pada ISO 27001:2013. Dengan adanya SOP penerapan keamanan informasi yang jelas dan terstruktur, organisasi dapat melindungi data dan sistem informasinya dengan lebih efektif dan mencegah insiden keamanan yang merugikan. SOP keamanan informasi yang terstruktur, organisasi juga dapat menerapkan langkah-langkah pencegahan dan pemulihan yang lebih cepat dan tepat dalam menghadapi insiden keamanan. SOP keamanan informasi juga memungkinkan organisasi untuk melakukan evaluasi dan perbaikan terhadap sistem keamanan informasi secara berkala untuk memastikan keamanan data dan sistem informasi selalu terjaga.

Pembagian kerja adalah proses membagi tugas dan tanggung jawab antara pegawai di dalam suatu organisasi untuk mencapai tujuan yang telah ditentukan. Pembagian kerja yang tepat dapat meningkatkan produktivitas dan efisiensi kerja dalam organisasi, serta memastikan bahwa setiap tugas dan tanggung jawab dikerjakan oleh orang yang tepat dengan keterampilan dan kemampuan yang sesuai.

3.2. Tingkat Kesiapan Penerapan Keamanan Informasi di Dinas Komunikasi dan Informatika Kota Madiun

Penulis melakukan pengukuran berdasarkan pada Indeks Keamanan Informasi (Indeks KAMI) 4.2 yang telah dilakukan pada Dinas Komunikasi dan Informatika Kota Madiun untuk menilai tingkat kesiapan dalam penerapan keamanan informasi



Gambar 1: Dashboard Indeks KAMI 4.2 Dinas Komunikasi dan Informatika Kota Madiun

Hasil dari penilaian Indeks KAMI tertera pada Dashboard siatas sebagai cerminan penilaian yang menampilkan status kesiapan pengamanan informasi berdasarkan ISO 27001. Menurut kepentingan penggunaan Sistem Elektronik di Dinas Komunikasi dan Informatika Kota Madiun, maka hasil dari penilaian tujuh area Indeks KAMI selanjutnya harus mendapatkan nilai diatas 583 untuk mendapatkan status baik, dalam penilaian yang telah dilakukan nilai yang didapatkan yaitu 624 dengan status kesiapan Baik. Hal ini mencerminkan tingkat pengelolaan keamanan informasi yang telah dilakukan pada Dinas Komunikasi dan Informatika Kota Madiun telah dikelola dengan baik. Dashboard hasil penilaian yang tertera pada Gambar 2 diatas dapat dijelaskan sebagai berikut :

1. Kategori sistem elektronik, Berdasarkan skor hasil yang didapat, maka tingkat penggunaan Sistem Elektronik memperoleh skor 40 yang mana ini masuk ke dalam kategori strategis. Kategori strategis skornya adalah diantara 35 hingga 50.

2. Area Tata Kelola Keamanan Informasi, Pada Area Tata Kelola Keamanan Informasi diperoleh skor total sebesar 118 yang mana memperoleh tingkat kematangan pada posisi III+ yang masuk ke kategori Terdefinisi dan Konsisten. Tingkat kematangan ini telah berada diatas ambang minimum kesiapan sertifikasi yang ada pada standar ISO/IEC 27001:2013.

3. Area Pengelolaan Risiko Keamanan Informasi, Hasil dari Area Pengelolaan Risiko Keamanan Informasi diperoleh skor 72 yang mana berdasarkan hasil skor tersebut, tingkat kematangan Pengelolaan Risiko Keamanan Informasi berada pada Tingkat V yang mana itu masuk dalam kategori optimal.

4. Area Kerangka Kerja Pengelolaan Keamanan Informasi, Hasil penilaian pada Area Kerangka Kerja Pengelolaan Keamanan Informasi diperoleh nilai evaluasi sebesar 152. Berdasarkan hasil skor tersebut, maka tingkat kematangan pada Area kerangka Kerja Pengelolaan Keamanan Informasi berada pada Tingkat III+ yang mana masuk ke kategori Terdefinisi dan Konsisten.

5. Area Pengelolaan Aset informasi, Hasil Penilaian pada Area Pengelolaan Aset Informasi diperoleh nilai sebesar 165 yang mana ini masuk ke dalam tingkat kematangan III yang masih masuk dalam kategori Terdefinisi dan Konsisten.

6. Area Teknologi dan Keamanan Informasi, Hasil skor penilaian pada Area Teknologi dan Keamanan Informasi diperoleh nilai total sebesar 117. Berdasarkan skor yang diperoleh Area Teknologi dan Keamanan Informasi berada pada Tingkat III+ yang masuk dalam kategori terdefinisi dan konsisten.

7. Area Suplemen, Area Suplemen ini terdiri dari tiga area kesiapan yaitu Pengamanan Keterlibatan Pihak Ketiga, Pengamanan Layanan Infrastruktur Awan dan Perlindungan Data Pribadi. Pada Pengamanan Keterlibatan Pihak Ketiga sebesar 100%, Pengamanan Layanan Infrastruktur Awan Sebesar 97% dan untuk perlindungan data pribadi sebesar 98%. Hasil yang diperoleh pada Area Suplemen ini tidak mempengaruhi tingkat kelengkapan serta kematangan pada area I hingga VI.

3.4. Diskusi Temuan Utama Penelitian

Pengelolaan persandian melihat aspek dari teori implementasi yang penulis gunakan sudah terpenuhi sesui standar dan indikator yang telah ditentukan melalui beberapa strategi Dinas Komunikasi dan Informatika Kota Madiun meski dalam pengelolaan baik tapi tetap terjadi beberpa ancaman terhadap keamanan informasi akan tetapi penanganan yang tepat dan ditanganni oleh tenaga ahli dapat mengatasi ancaman tersebut dan tidak terjadi kerugian. Pengelolaan persandian yang baik berdampak kualitas pelayanan informasi kepada masyarakat. Berbeda dengan temuan penelitian sebelumnya karena hasil evaluasi akhir Indeks KAMI yang memperoleh skor akhir 624 berdasarkan gambar menunjukkan bahwa status kesiapan pengamanan informasi Dinas Komunikasi dan Informatika Kota Madiun termasuk dalam status kesiapan Baik karena mendapatkan nilai diatas 583.

4.5. Diskusi Temuan Menarik Lainnya (opsional)

Penulis menemukan bahwa meskipun pengelolaan persandian di Dinas Komunikasi dan Informatika Kota Madiun telah dilaksanakan dengan baik dan sesuai dengan SOP, akan tetapi tetap ada peluang terjadinya gangguan. Penulis menemukan bahwa saat ini marak terjadi serangan denga nisi konten iklan judi online yang menyusupi website pemerintahan meskipun begitu serangan yang terjadi dapat diatasi dengan cepat dan tepat.

IV. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan oleh peneliti mengenai pengelolaan persandian dalam rangka keamanan informasi di Dinas Komunikasi dan Informatika Kota Madiun. Pengelolaan

Persandian telah dilaksanakan secara maksimal namun dalam prakteknya dilapangan tetap ada celah yang disusupi oleh pihak yang tidak bertanggung jawab untuk menyusup pada system yang ada. Berdasarkan penelitian yang telah dilakukan oleh peneliti berdasarkan pada Teori Edward III, maka dapat ditarik kesimpulan sebagai berikut:

1. Komunikasi, dalam penyampaian informasi mengenai pengelolaan keamanan informasi antara pimpinan kepada pegawai pada Seksi Keamanan Informasi dan Persandian dilakukan melalui SIKD, rapat dan juga pesan singkat telah berjalan dengan baik.
2. Sumber Daya, dalam hal pekerjaan pegawai telah bekerja dengan baik baik dalam koordinasi maupun menjalankan SOP sudah sesuai dengan petunjuk. Akan tetapi terjadinya permasalahan tidak bisa dihindari seperti adanya penyusup dalam sistem yang terjadi secara mendadak. Oleh karena itu pegawai dalam merespon hal ini bertindak secara sesuai dengan SOP.
3. Disposisi, pegawai yang melaksanakan tugas memiliki disposisi yang baik dan telah menjalankan pengelolaan persandian dengan baik seperti yang diinginkan oleh atasan berdasar pada ISO 27001:2013. Dalam menjalankan disposisi membuat pengelolaan persandian menjadi lebih efektif.
4. Struktur Birokasi, dalam melaksanakan tugas para pegawai pada Seksi Keamanan Informasi dan Persandian pegawai bekerja sama saling bantu membantu menghilangkan ego sectoral dan juga tanggung jawab yang diemban menjadi tanggung jawab Bersama.

Hasil dari evaluasi akhir pada tingkat pengelolaan keamanan informasi di Dinas Komunikasi Kota Madiun, dilihat dari dashboard maka diperoleh hasil evaluasinya adalah “Baik” dengan perolehan skor Tingkat Kelengkapan Penerapan Standar ISO 27001:2013 sebesar 624 dari 645 dan tingkat kematangan berada pada tingkat III s/d V.

Keterbatasan Penelitian. Penelitian ini memiliki keterbatasan utama yakni waktu dan biaya penelitian. sumber rujukan penelitian persandian termasuk acuan penelitian pengamanan informasi pemerintah daerah

Arah Masa Depan Penelitian (*future work*). Penulis menyadari masih awalnya temuan penelitian, oleh karena itu penulis menyarankan agar dapat dilakukan penelitian lanjutan pada lokasi serupa berkaitan dengan pengelolaan persandian karena semakin berkembangnya teknologi maka keamanan informasi juga akan semakin berkembang sehingga pembaca juga dapat mengikuti perkembangan tersebut.

V. UCAPAN TERIMA KASIH

Ucapan terima kasih terutama ditujukan kepada Kepala Dinas Komunikasi dan Informatika Kota Madiun beserta seluruh pegawai di lingkungan dinas dan juga seluruh elemen yang berjasa mendukung hingga penulis dapat menyelesaikan penyusunan tulisan ini.

VI. DAFTAR PUSTAKA

Basyarahil, F. A. (2017). *Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berbasis ISO/IEC 27001:2013 di Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya*. ITS Surabaya.

Creswell, J. W. (2014). *Research Design: Pendekatan Kualitatif, Kuantitatif dan Mixed* (3rd ed.). Pustaka Pelajar.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, *04*(02), 92–100. https://doi.org/10.4236/jis.2013.42011

Iqbal, M. (2021). *EVALUASI KEAMANAN SISTEM INFORMASI RSUD ARIFINACHMAD PEKANBARU MENGGUNAKAN ISO 27001*.

Octaviani, S. I. D. (2019). *Evaluasi Kesiapan Kerangka Kerja Keamanan Informasi Pada Dinas Komunikasi dan Informatika Kota Batu Dengan Menggunakan Indeks KAMI*. Universitas Brawijaya.

Pratama, E. R. (2018). *Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi dengan Menggunakan Indeks KAMI dan ISO 27001 (Studi Kasus KOMINFO Provinsi Jawa Timur)*. Universitas Brawijaya.

Setiawan, H., & Mustofa, K. (2013). Metode Audit Tata Kelola Teknologi Informasi di Instansi Pemerintah Indonesia Audit Method for Information Technology Governance in Indonesian Government Agencies. *IPTEK-KOM*, *15*(1), 1–15.

Slamet, M. R., Wulandari, F., & Amalia, D. (2019). PENILAIAN PENGAMANAN TEKNOLOGI PADA SISTEM PEMBELAJARAN ELEKTRONIK MENGGUNAKAN INDEKS KEAMANAN INFORMASI DI POLITEKNIK NEGERI BATAM. *JOURNAL OF APPLIED BUSINESS ADMINISTRATION*, *3*(1), 162–171. https://doi.org/10.30871/jaba.v3i1.1305

Sudjiman, P. E., & Sudjiman, L. S. (2018). *ANALISIS SISTEM INFORMASI MANAJEMEN BERBASIS KOMPUTER DALAM PROSES PENGAMBILAN KEPUTUSAN*.