p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom

AUDIT KEAMANAN SISTEM INFORMASI TRAFFIC COUNTING MENGGUNAKAN FRAMEWORK ISO 27002:2022 (STUDI KASUS: DINAS PERHUBUNGAN KABUPATEN SUBANG).

Lutfia Meidiana[1], Tazkia Salsabila Ardan[2]

Fakultas Ilmu computer, Universitas Subang[1,2]

Alamat email

tazkiaardan@unsub.ac.id

Abstract

Sistem Traffic Counting adalah suatu sistem berbasis web yang dikembangkan oleh Dinas Perhubungan Kabupaten Subang dengan tujuan Dinas Perhubungan Kabupaten Subang pada Bidang Lalu Lintas untuk memudahkan mengumpulkan data lalu lintas kendaran roda dua dan roda empat dan kondisi lalu lintas yang manfaatnya untuk mengukur kinerja kondisi jalan lancar atau padat dan membuat manajemen rekayasa lalu lintas. Oleh karena itu perlu adanya upaya serius untuk mengidentifikasi dan mengatasi potensi kerentanan dalam Sistem Traffic Counting agar menjamin kerahasiaan, integritas dan ketersedian informasi, dan juga kinerja sistem yang harus dikendalikan agar dapat berjalan dengan optimal. Standar yang digunakan dalam proses audit ISO 27002:2022 dengan klausul 7. Physical Controls, dan 8. Technological Controls yang difokuskan membahas keamanan fisik dan keamanan teknlogi. Setelah dilakukan analisis, hasil perhitungan Klausul 7 dan klausul 8 yang dimiliki oleh Dinas Perhubungan Kabupaten Subang Berada di Level 3 (Defined) Hasil dari proses perhitungan dengan jumlah rata-rata control objektif pada Klausul 7 (keamanan fisik) adalah 3,47 dan Klausul 8 (Teknlogi Kontrol) adalah 3,25. Sedangkan harapan Dinas Perhubungan Kabupaten Subang ada di level 5, maka peningkatan level ini dapat dilakukan dengan menerapkan aktivitas yang belum dilakukan oleh Organisasi hingga mencapai level yang diharapkan. Penelitian ini hasilnya sampai ke temuan dan memberikan rekomendasi perbaikan kepada Organisasi.

Keywords: *Audit, Sistem, Traffic Counting, ISO 27002:2022, lalu lintas*

PENDAHULUAN

Transportasi telah menjadi kebutuhan dasar masyarakat serta menjadi komponen utama dalam menunjang kehidupan masyarakat. Salah satu masalah klasik yang sering terjadi terutama di kota-kota besar adalah kemacetan. Informasi terkait dengan jumlah kendaraan yang melintas di ruas jalan menjadi salah satu hal yang penting. Salah satu penyebab terjadinya hal demikian adalah disebabkan karena tidak sesuainya daya tampung jalur jalan

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom

dengan jumlah kendaraan yang akan melewati Jalan ruas Kota Subang serta cara yang digunakan oleh pihak yang terkait untuk melakukan proses perhitungan kendaraan.

Dinas Perhubungan Kabupaten Subang terbagi menjadi 3 bidang yaitu bidang lalu lintas, bidang angkutan darat dan sarana jalan, bidang teknik sarana dan prasarana. Dari semua bidang-bidang ini memiliki tugas berbeda. Dinas Perhubungan terdapat salah satu bidang Lalu Lintas (Lalin) yang bertugas melaksanakan rencana kerja terkait dengan manajemen rekayasa lalu lintas, Menyusun kebijakan teknis terkait lalu lintas, termasuk pengaturan dan pengendalian. mengevaluasi hasil, dan menyusun laporan terkait lalu lintas. Sistem Traffic Counting ini diintegrasikan dengan CCTV Area Traffic Control System (ATCS) pada 9 Simpang Kota Subang. Sistem Traffic Counting bertujuan Dinas Perhubungan Kabupaten Subang pada Bidang Lalu Lintas untuk memudahkan mengumpulkan data lalu lintas kendaran roda dua dan roda empat dan kondisi lalu lintas yang manfaatnya untuk mengukur kinerja kondisi jalan lancar atau padat dan membuat manajemen rekayasa lalu lintas. Berdasarkan hasil observasi dan wawancara dengan Operator ATCS, diketahui bahwa Sistem Traffic Counting yang mereka miliki pernah terjadinya penyerangan menargetkan server dan menggangu layanan jaringan sehingga server down, website tidak bisa diakses dan data Traffic Counting tidak bisa membaca kendaraan, yang mengakibatkan menghambat kinerja pegawai selain itu juga data jumlah kendaraan tidak bisa ditampilkan, dan pernah terjadinya kebocoran data karena keamanan teknologi merupakan kebutuhan yang penting bagi organisasi agar menjamin kerahasiaan,integritas dan ketersedian informasi, selain itu juga sistem informasi ini juga belum pernah dilakukan audit.

Ada banyak standar yang dapat dilakukan dalam mengukur keamanan Teknlogi Informasi, contoh yang sering ditemui dalah International Organization for Standardization (ISO). ISO 27002 adalah standar internasional untuk kontrol keamanan informasi. Standar ini memberi panduan untuk organisasi yang ingin melindungi informasi mereka dari ancaman siber. Standar ini berisi daftar kontrol yang dapat dipilih dan diterapkan sesuai dengan kebutuhan organisasi. Standar ISO 27002 Tahun ini mengeluarkan versi terbaru, yakni versi 2022. Pembaruan terbaru ini ISO 27002:2022 terdapat 4 klausul (5. Organization Controls, 6. People Controls, 7. Physical Controls, dan 8. Technological Controls). Klausul yang penulis gunakan pada penelitian ini adalah klausul 7 Physical Control (pengendalian secara fisik) mencakup 14 sub klausul yang digunakan penulis 7 sub klausul dan 8 Technological Control (Teknlogi Kontrol), mencakup 34 sub klausul yang digunakan penulis 5 sub klausul. Oleh karena itu, perlu adanya upaya serius untuk mengidentifikasi dan mengatasi potensi kerentanan dalam Sistem Traffic Counting. Membuat peneliti berminat melakukan penelitian

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom

terhadap keamanan Sistem Traffic Counting untuk meminimalisir terjadinya hal-hal yang tidak diinginkan.

KAJIAN TEORI

SISTEM INFORMASI

Leitch dan Davis dalam (Ermana et al., 2012) Sistem Informasi (SI) adalah sistem dalam sebuah organisasi yang menghubungkan kebutuhan pengolahan transaksi sehari-hari, mendukung operasi, manajerial, dan strategi organisasi, serta memberikan laporan kepada pihak eksternal yang diperlukan.

KEAMANAN INFORMASI

Menurut *Sarno & Iffano* Menjelaskan Keamanan informasi adalah menjaga informasi dari ancaman/bahaya yang ditakutkan atau yang mungkin terjadi untuk menjamin dan memastikan kelangsungan bisnis (*business continuity*), meminimasi resiko bisnis (*reduce business risk*) dan memaksimalkan atau mempercepat pengambilan inventasi dan peluang bisnis. (Muhammad Reza Hamzah, n.d 2013).

Menurut Whitman dan Mattord (2009) dalam (Windriya, 2013) Perlindungan pada Informasi tersebut dilakukan untuk memenuhi aspek keamanan informasi. Aspek-aspek tersebut seharusnya diperhatikan atau dikontrol dan semestinya dipahami untuk diterapkan beberapa aspek yang terkait dengan keamanan informasi yang akan dijelaskan sebagai berikut:

a. *Privacy* Informasi yang dikumpulkan, digunakan, dan disimpan oleh organisasi adalah dipergunakan hanya untuk tujuan tertentu, khusus bagi pemilik data saat informasi ini dikumpulkan. *Privacy* menjamin keamanan data bagi pemilik informasi dari orang lain.
b. *Identification* Sistem informasi memiliki karakteristik identifikasi jika bisa mengenali penggunaannya. Identifikasi adalah langkah pertama dalam memperoleh hak akses ke informasi yang diamankan. Identifikasi umumnya dilakukan dengan penggunaan user name dan user ID.
c. *Authentication* Autentikasi terjadi pada saat sistem dapat membuktikan bahwa pengguna memang benar-benar orang yang memiliki identitas yang di klaim.
d. *Authorization* Setelah identitas pengguna diautentikasi, sebuah proses yang disebut autorisasi memberikan jaminan bahwa pengguna (manusia dan komputer) telah mendapatkan autorisasi secara spesifik dan jelas untuk mengakses, mengubah, atau menghapus isi dari informasi.

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom

e. *Accountability* Karakteristik ini dipenuhi jika sebuah sistem dapat menyajikan data semua aktivitas terhadap informasi yang telah dilakukan, dan siapa yang melakukan aktivitas itu.

AUDIT SISTEM INFORMASI

Menurut (Widayanti & Purnawati, 2013) Menjelaskan Audit adalah kegiatan suatu memeriksa suatu entitas, kemudian dengan mengumpulkan bukti/data dan mengevaluasi bukti/data tersebut berdasarkan standar/kriteria yang telah ditetapkan, kemudian akan menghasilkan laporan dari auditor mengenai kesesuaian kegiatan atau kejadian yang diperiksa tersebut dengan kriteria yang ditetapkan (Muhammad Reza Hamzah, n.d 2013).

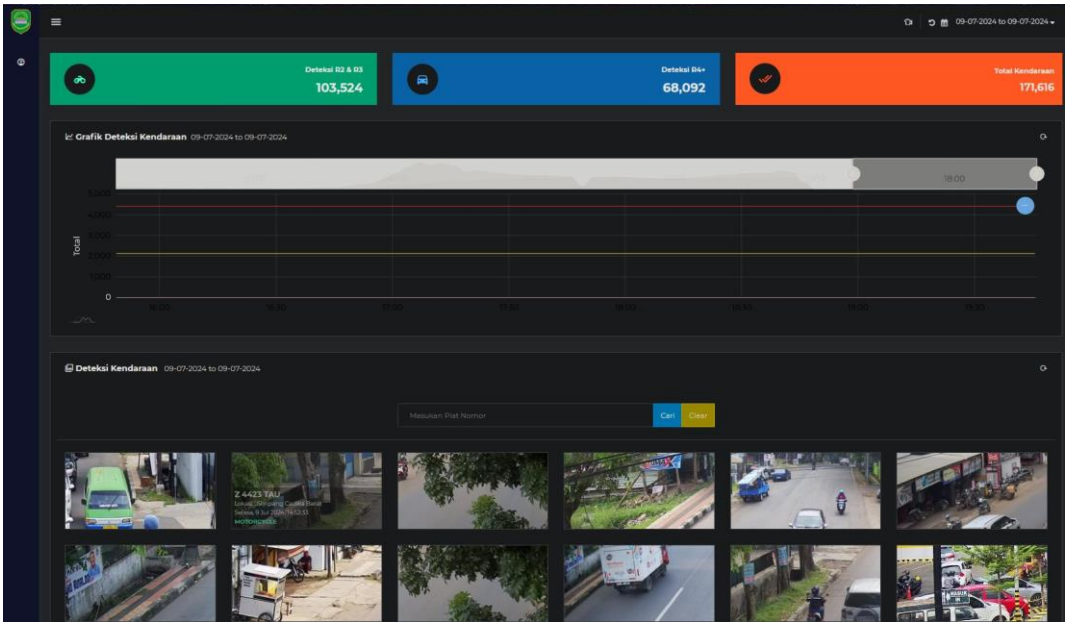
Menurut (Taryana & Ardan, 2024) Audit pada dasarnya adalah proses sistematis dan obyektif dalam memperoleh dan mengevaluasi bukti-bukti tindakan ekonomi, guna memberikan asersi/pernyataan dan menilai seberapa jauh tindakan ekonomi sudah sesuai dengan kriteria yang berlaku dan mengkomunikasikan hasilnya kepada pihak terkait.

Weber dalam (Ermana et al., 2012) mendefinisikan Audit Sistem Informasi sebagai proses pengumpulan dan pengevaluasian bukti (evidence) untuk menentukan apakah sistem informasi dapat melindungi aset, serta apakah teknologi informasi yang ada telah memelihara integritas data sehingga keduanya dapat diarahkan kepada pencapaian tujuan bisnis secara efektif dengan menggunakan sumber daya secara efektif.

TRAFFIC COUNTING

Traffic Counting adalah aplikasi web yang dikembangkan oleh Dinas Perhhubungan Kabupaten Subang untuk Traffic Counting adalah sistem berbasis web yang mengumpulkan data pergerakan kendaraan di jalan raya. Dengan pemasangan kamera berbasis mikrokontroler di setiap persimpangan, sistem ini mengamati kendaraan yang memasuki 9 Simpang Kota Subang. Hasilnya berupa data kendaraan roda dua dan roda empat serta grafik per menit dan per jam. Manfaatnya termasuk penghitungan efektif secara real-time tanpa perlu perhitungan manual, antisipasi lonjakan volume kendaraan saat liburan, dan manajemen lalu lintas. Sistem ini juga membantu mengukur kinerja kondisi jalan dan menyusun kebijakan teknis terkait lalu lintas. Dalam konteks audit aplikasi, analisis dilakukan untuk mengevaluasi berbagai aspek seperti keamanan data, efisiensi proses, dan kegunaan fitur, sejauh mana aplikasi ini memenuhi kebutuhan pengguna ataupun tingkat keamananya

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom



Gambar 1 Dashboard Sistem Traffice Counting

ISO 27002:2022

ISO 27002:2022 adalah standar yang memberikan saran untuk mengelola kontrol keamanan informasi dalam organisasi. Standar ini berlandaskan pada sistem manajemen keamanan informasi (SMKI) yang diuraikan dalam ISO 27001:2013. Standar ini telah diperbarui pada tahun 2022. Edisi sebelumnya adalah ISO 27002:2013. Standar ISO 27002 ini berisi 93 kontrol keamanan informasi yang dibagi menjadi 4 kategori utama, yaitu (5. Organization Control, 6. People control, 7. Physical control dan 8. Technological Control) kontrol-kontrol ini dapat disesuaikan dengan konteks bisnis organisasi.

Standar ini dapat digunakan sebagai acuan untuk melakukan audit sistem informasi dalam suatu organisasi. Audit sistem informasi dengan menggunakan ISO 27002:2022 bertujuan untuk menilai sejauh mana suatu organisasi telah menerapkan pengendalian keamanan informasi yang sesuai dengan standar tersebut. Audit sistem informasi dengan menggunakan ISO 27002:2022 juga dapat membantu organisasi untuk meningkatkan kualitas dan kinerja sistem informasinya.

SKALA LIKERT

Menurut (Sugiyono, 2010), tujuan dari skala Likert adalah untuk mengukur sikap setiap orang dalam dimensi yang sama dan menempatkan mereka ke arah satu kontinuitas dari butir soal. Skala Likert biasanya menggunakan kategori skor dari 1 hingga 5 dengan penilaian skor untuk setiap angka seperti yang ditunjukkan dalam tabel 5 berikut:

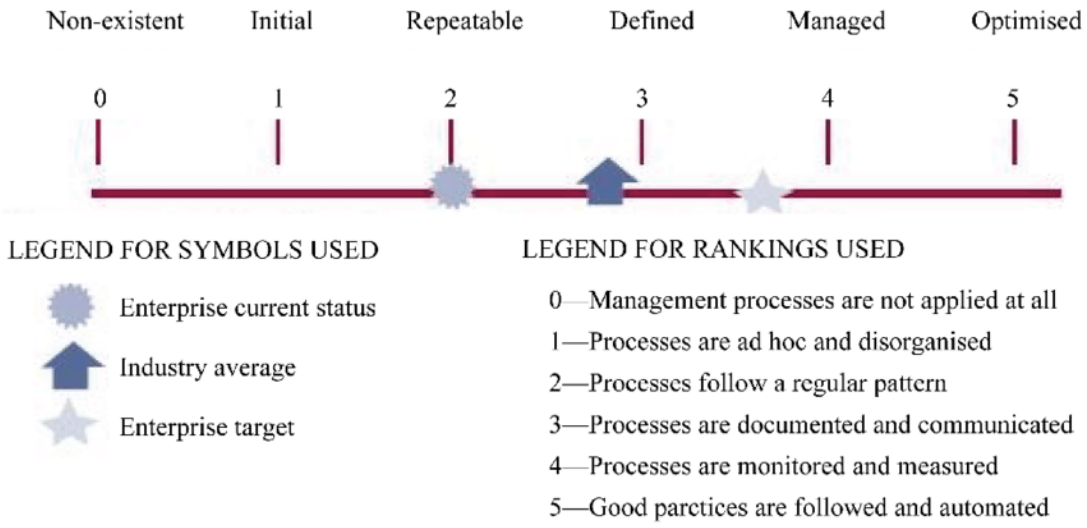
p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom

Tabel 1 Skala Likert

Pernyataann	Skor
Sangat Setuju (SS)	5
Setuju (S)	4
Kurang Setuju (KS)	3
Tidak Setuju (TS)	2
Sangat Tidak Setuju (STS)	1

MATURITY MODEL

Menurut (Sari, 2020) Maturity Model adalah alat yang mewakili jalur menuju yang semakin terorganisir dan cara sistematis untuk melakukan bisnis yang biasanya melibatkan orang, organisasi, dan proses. Dalam model kedewasaan, jalur evolusi dijelaskan melalui tahapan yang berbeda, untuk mencapai tingkat berikutnya memerlukan pencapaian tujuan pada tingkat yang diinginkan dan semua tingkat sebelumnya. Pengukuran kematangan risiko perlu dilakukan untuk mengetahui apakah penerapan manajemen risiko pada organisasi berhasil atau tidak.



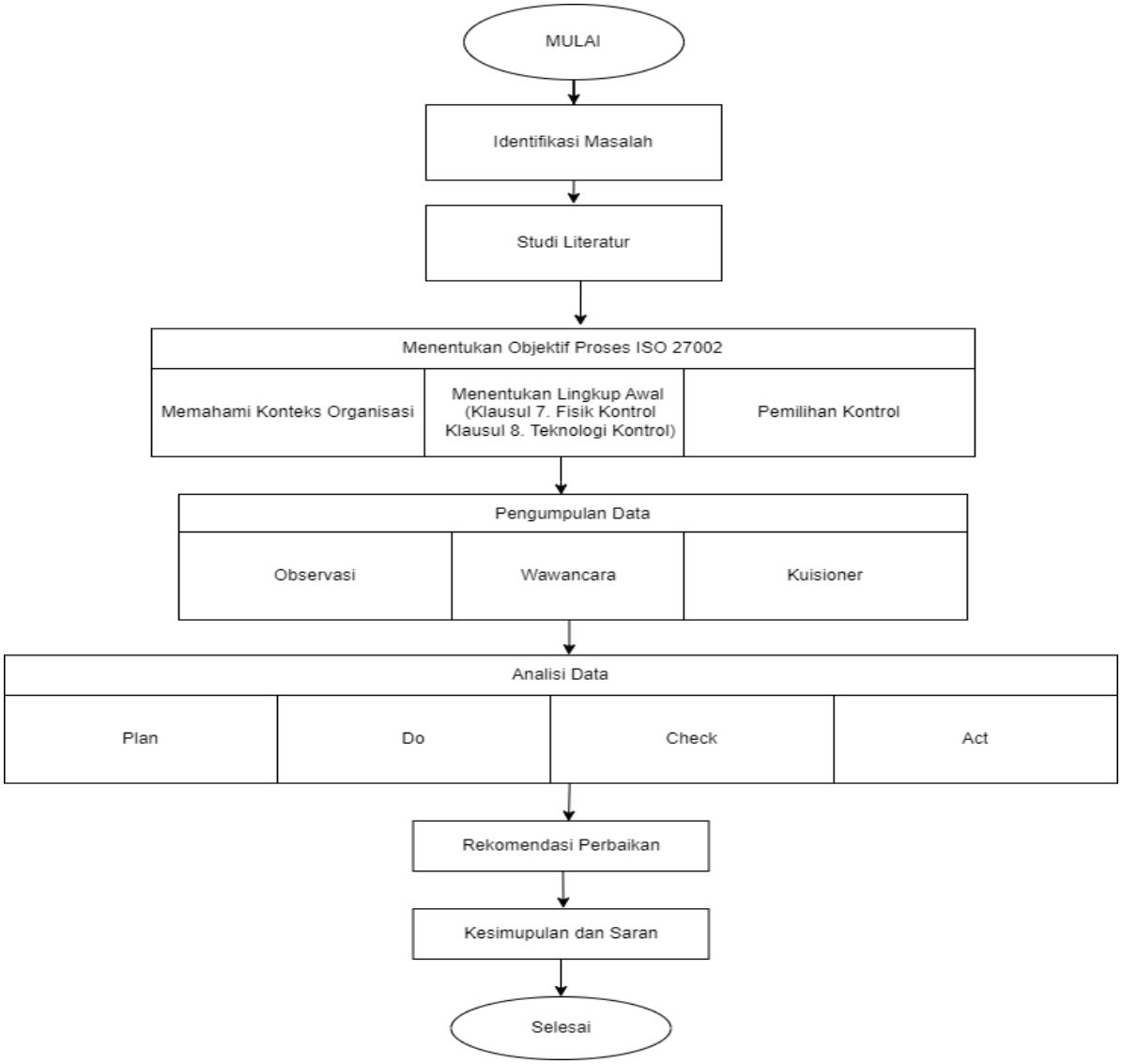
Gambar 2 Maturity Model

Sumber : https://netsolution.co.id/asesmen-audit-it-maturity-level/

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom

METODE PENELITIAN

Dalam penelitian ini, data berasal dari dua macam sumber, yaitu data primer dan data sekunder. Data primer adalah data yang diperoleh langsung dari sumber pertama. Data sekunder adalah data yang diperoleh dari sumber lain yang sudah ada sebelumnya.



Gambar 3 Metode Penelitian

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom

HASIL DAN PEMBAHASAN

1. IDENTIFIKASI ANCAMAN DAN KERENTANAN

Berikut adalah tabel identifikasi ancaman dan kerentanan (Risk Assessment) untuk aset:

Tabel 2 Penilain Resiko (Risk Assement)

No	Aset	Ancaman yang bisa terjadi	Kerentanan	Dampak Potensial	Kemungkinan Terjadi
1	Server	Serangan Siber, Perusakan/sabotase	Konfigurasi tidak aman, patch tidak terpasang, pengamanan fisik lemah, Password lemah,	Data hilang, downtime, kebocoran informasi	Sedang
2	DVR dan NVR	Hacking, sabotase	Konfigurasi tidak aman, Koneksi internet tidak aman, Firmware tidak update, pengamanan fisik lemah	Hilangnya rekaman penting,	Tinggi
3	Video Processor	Serangan siber, sabotase	Firmware tidak update, pengamanan fisik lemah	Kehilangan Data	Sedang
4	PC	Malware, phishing, sabotase	Antivirus tidak update, user awareness rendah	Kehilangan data, penyebaran malware	Sedang
5	UPS	Sabotase, Human Error	Pemeliharaan tidak memadai.	Kerusakan pada kelistrikan sehingga mengakibatkan perangkat rusak.	Sedang
6	Perangkat Jaringan	Serangan DDoS, hacking, sabotase	Password lemah, pengaturan keamanan standar	Kegagalan jaringan, kehilangan konektivitas	Tinggi
7	Pengkabelan Listrik dan Jaringan	Sabotase, Human Error	Instalasi tidak sesuai standar, akses tidak terbatas	Gangguan operasi, potensi kebakaran	Rendah
8	Doorlock System (kontrol masuk ruangan)	Hacking, sabotase	Sistem tidak dienkripsi, akses tidak sah	Akses tidak sah, ancaman keamanan fisik	Tinggi

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom

2. PENENTUAN KLAUSUL DAN KONTROL

Penelitian ini berfokus pada klausul 7 Physical Control (Fisik Kontrol), Mencakup 14 Sub klausul yang digunakan penulis 7 sub klausul dan 8 Technological Control (Teknlogi Kontrol), mencakup 34 sub klausul tetapi yang digunakan penulis hanya 5 Sub Klausul yang akan ditampilkan dalam tabel berikut:

Tabel 3 Klausul Yang Digunakan

Klausul	ISO/IEC 27002:2022	Nama Kontrol
7. Fisik Kontrol	7.2	Kontrol Masuk Fisik
	7.4	Pemantauan Keamanan Fisik
	7.5	Perlindungan Terhadap Ancaman Fisik Dan Lingkungan
	7.6	Bekerja Diwilayah Aman
	7.7	Kebersihan Meja
	7.12	Keamanan Pengkabelan
	7.13	Pemeliharaan Peralatan
8. Teknologi Kontrol	8.6	Manajemen Kapasitas
	8.7	Perlindungan Terhadap Malware
	8.12	Pencegaham Kebocoran Data
	8.13	Pencadangan Informasi
	8.20	Keamanan Jaringan

3. HASIL TEMUAN MATURITY LEVEL

Tabel 4 Hasil Maturity Level Klausul 7 Keamanan Fisik

Klausul	Objektif Kontrol	Tingkat Kemampuan	Rata-Rata Objektif Kontrol
Klausul 7 (Keamanan Fisik)	7.2 Kontrol Masuk Fisik	4,5	3,47
	7.4 Pemantauan Keamanan fisik	2,5	
	7.5 Perlindungan Terhadap Ancaman Fisik Dan Lingkungan	2,66	
	7.6 Bekerja Di Wilayah Aman	3,66	
	7.7 Kebersihan Meja Kerja	3,33	
	7.12 Keamanan Pengkabelan	3,33	
	7.13 Pemeliharan Perlatan	4,33	
	Maturity Level Klausul 7		3,47

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom

Tabel 5 Hasil Maturity Level Klausul 8 Teknlogi Kontrol

Klausul	Objektif Kontrol	Tingkat Kemampuan	Rata-Rata Objektif Kontrol
Klausul 8 (Teknologi Kontrol)	8.6 Manajemen Kapasitas	4.5	3,25
	8.7 Perlindungan Terhadap Malware	3	
	8.12 Pencegahan Kebocoran Data	4	
	8.13 Pencadangan Informasi	2	
	8.20 Keamanan Jaringan	2,75	
	Maturity Level Klausul 8		3,25

Hasil dari proses perhitungan tingkat kematangan Klausul 7 (keamanan fisik) adalah 3,47 dan Klausul 8 (Teknlogi Kontrol) adalah 3,25, yang berarti defined. Hal ini menunjukkan bahwa kontrol proses telah dilaksanakan dengan baik dan terdapat acuan pelaksanaannya, tetapi tidak ada pengukuran kepatuhan. dan kontrol memerlukan perbaikan lebih lanjut untuk mencapai tingkat kepatuhan yang diperlukan. Hal ini dapat dilihat dari beberapa prosedur yang belum tercatat secara formal dan beberapa kontrol yang belum dilakukan secara optimal dan perlu diperhatikan, pada klausul 7 Fisik Kontrol yaitu keamanan pemantauan keamanan fisik, perlindungan terhadap ancaman fisik dan lingkungan, kebersihan meja kerja, keamanan pengkabelan, bekerja diwilayah aman, pada klausul 8 Teknlogi Kontrol yaitu keamanan perlindungan terhadap malware, pencadangan informasi dan keamanan jaringan. Hasil perhitungan tersebut dapat dilihat dari tabel diatas.

4. HASIL LAPORAN AUDIT

Dari hasil audit keamanan teknologi informasi pada Dinas Perhubungan yang telah dilakukan, maka didapatkan kesimpulannya berupa: 1. Penerapan ISO 27002 Klausul 7 keamanan fisik dan Klausul 8 Teknlogi Kontrol pada keamanan teknologi informasi pada Bidang Lalu Lintas Dinas Perhubungan Kabupaten Subang telah dilakukan dengan baik, meskipun belum maksimal namun beberapa objek kontrol yang ada di Klausul 7 dan Klausul 8 sudah diterapkan. 2. Kebocoran data yang terjadi merupakan akibat darinya tidak ada kebijakan dan ketentuan, pastikan semua orang yang berkepentingan terdaftar pada sistem doorlock.	Maturity Rating Klausul 7 Fisik Kontrol: 3.47 Klausul 8 Teknlogi Kontrol: 3.25 Audit Isu 1. Adanya kasus Kebocoran data/penyebaran data. 2. Adanya kasus kehilangan asset akibat kurangya keamanan kontrol masuk fisik

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom

Perlunya menerapkan kegiatan pencatatan log aktivitas pada sistem doorlock, catat setiap akses masuk dan keluar, termasuk waktu dan identitas pengguna. Pastikan petugas selalu memantau tamu yang berkunjung dan Tingkatkan pemeriksaan terhadap barang-barang yang tidak boleh dibawa oleh tamu dan anggota sekalipun yang tidak berkepentingan saat memasuki ruangan. Selain itu Perlunya penerapan otentikasi yang lebih kuat, seperti otentikasi dua ketika (misalnya, kombinasi kata sandi dan token) untuk memastikan hanya pengguna yang berwenang yang dapat mengakses data. Dan buatkan pencatatan/logging ketika adanya penyalinan data dan selalu memeriksa pencatatan/logging untuk mencegah kebocoran data, selain itu berikan akses ke beberapa anggota yang dipercaya terkait penyalinan data selain itu perlunya pemasangan CCTV didalam ruangan kerja. 3. Kasus kehilangan asset yang terjadi akibat kurangnya keamanan keamanan kontrol masuk fisik, tidak adanya pemeriksaan baik keluar/masuk pada area kerja sensitive selain itu perlunya penyimpanan khusus, pemasangan doorlock atau penguncian kunci fisik. Untuk menyimpan asset untuk mengantisipasi kehilangan asset Kembali kemudian pasang CCTV di dalam area sensitive/pada ruangan asset tersebut. 4. Kasus yg terjadi ruangan server pecah/retak Kurangnya keamanan perlindungan terhadap ancaman fisik dan lingkungan. Jadi perlunya untuk untuk memasangan perangkat detector untuk mengantisipasi penyusup masuk atau faktor lingkungan kemudian pasang CCTV pada area blankspot yang jarang untuk dilalui untuk mengidentifikasi akibat retak/pecah tersebut. 5. Kasus yg terjadi kasus serangan dunia maya DOS *(Denial of Service)* yang mengakibatkan server down. Merupakan akibat kurangnya Pemantauan rutin dari Jaringan, perangkat keras dan konfigurasi. Perlu melakukan merekrut anggota/karyawan/tenaga ahli internal dengan skill khusus didalam organisasi/instansi untuk selalu standby ketika ada trouble. 6. Kurangnya perawatan Perangkat keras Baik itu CCTV alat pendukung CCTV, PC, Server, Alat jaringan, Keamanan Kabel, dan manajemen kabel. 7. Di organisasi/Intansi Terdapat beberapa objek kontrol yang diterapkan namun belum memiliki kebijakan dan prosedur yang terdokumentasi, bahkan ada beberapa tindakan yang dilakukan hanya karna spontanitas tanpa adanya aturan yang jelas yang bersifat secara formal.	menganai Asset didalam ruangan kerja 3. Adanya kasus ruangan server pecah/retak kurangnya Keamanan ancaman Fisik dan perlindungan terhadap lingkungan. 4. Kurangnya keamanan pemantauan ataupun konfigurasi mengenai perangkat keras jaringan dikarenakan adanya kasus serangan dunia maya DOS *(Denial of Service)* yang mengakibatkan server down. 5. Belum memiliki aturan dan prosedur formal terhadap kebijakan yang ada

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom

PENUTUP

SIMPULAN

Berdasarkan hasil dan pembahasan yang sudah dijelaskan di Bab sebelumnya, peneliti menyimpulkan bahwa :

1. Hasil yang didapatkan dari analisis tingkat kematangan (*maturity level*) pada klausul 7 Fisik Kontrol yaitu 3,47 (defined) dan Klausul 8 Teknlogi Kontrol 3,25 (defined) berada pada level 3.
2. Tingkat keamanan teknologi informasi yang dimiliki Dinas Perhubungan Kabupaten Subang sudah cukup baik namun kebijakan dan prosedur yang sekarang dilaksanakan belum memenuhi kepatuhan aspek standard keamanan ISO 27002:2022.

SARAN

Berdasarkan hasil penelitian yang dilakukan, peneliti memberikan rekomendasi yang diharapkan kedepannya bagi Organisasi/Instansi untuk mencapai tingkat yang diharapkan, antara lain:

1. Perlu adanya evaluasi Penilaian keamanan teknologi informasi terkait teknologi informasi perlu dilakukan secara berkala untuk meningkatkan keamanan teknologi informasi khususnya pada aspek fisik dan aspek teknolgi.
2. Untuk mencapai peningkatan yang diharapkan dalam keamanan teknologi informasi di Dinas Perhubungan Kabupaten Subang, Terapkan seluruh rekomendasi yang sudah ditulis diatas.

DAFTAR PUSTAKA

Ermana, F., Tanuwijaya, H., & Mastan, I. A. (2012). Audit Keamanan Sistem Informasi Berdasarkan Standar Iso 27001 pada PT. BPR JATIM. *Jurnal Sistem Informasi Dan Komputer Akuntansi*, *1*(1).

Febrianto, F. (n.d.). *EVALUASI KEAMANAN INFORMASI MENGGUNAKAN ISO/IEC 27002: STUDI KASUS PADA STIMIK TUNAS BANGSA BANJARNEGARA*.

Muchsam, Y., Falahah, F., & Saputro, G. I. (2011). Penerapan gap analysis pada pengembangan sistem pendukung keputusan penilaian kinerja karyawan (studi kasus pt. xyz). *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*.

Muhammad Reza Hamzah. (n.d.). *MUHAMMAD REZA HAMZAH - FST*. Retrieved October 9, 2023, from https://repository.uinjkt.ac.id/dspace/handle/123456789/68155

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom

Sari, W. (2020). Risk Maturity Level dan Upaya Peningkatannya. *Karya Ilmiah Online Universitas Trisakti*.

Sugiyono, P. D. (2010). Metode Peneliian. *Kuantitatif, Kualitatif, Dan R&D*.

Taryana, K., & Ardan, T. S. (2024). *AUDIT TATA KELOLA SISTEM INFORMASI MANAGEMENT ASSET PADA YAYASAN AS-SYIFA AL-KHOERIYYAH MENGGUNAKAN FRAMEWORK COBIT 2019* (Vol. 11, Issue 1). http://ejournal.unsub.ac.id/index.php/Fasilkom

Windriya, D. R. (2013). *TA: Audit Keamanan Sistem Informasi pada Instalasi Sistem Informasi Manajemen RSUD Bangil Berdasarkan ISO 27002*. Stikom Surabaya. https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en