Journal of Applied Informatics and Computing (JAIC)
Vol.x, No.x, Juli 201x, pp. xx~xx
e-ISSN: 2548-6861

Analysis of Cybersecurity Maturity Level at PT XYZ Using Cyber Security Maturity (CSM)

(*Analisis Tingkat Kematangan Keamanan Siber Pada PT XYZ Menggunakan Cyber Security Maturity (CSM)*)

Cut Isnaini Mardziyyah
Teknik Informatika, Politeknik Negeri Batam
Jl. Ahmad Yani, Tlk. Tering, Kec. Batam Kota, Kota Batam, Kepulauan Riau 29461
cut.4332011006@students.polibatam.ac.id

Article Info

Article history:

Received …
Revised …
Accepted …

Keyword:

CSM, Cyber Security Maturity.

ABSTRACT

In an effort to enhance cybersecurity at PT XYZ, a Cyber Security Maturity (CSM) analysis was conducted. This assessment identified the level of cybersecurity maturity and highlighted strengths and weaknesses across various aspects. The results indicate that PT XYZ's cybersecurity still requires improvement. Although there are structured organizations and procedures in place, the implementation of cybersecurity is still inconsistent, potentially increasing cybersecurity risks. This analysis provides a better understanding of PT XYZ's cybersecurity condition and encourages improvement plans to strengthen their cybersecurity.

I. PENDAHULUAN

Perkembangan teknologi informasi, terutama dalam era digital, memberikan dampak signifikan pada berbagai aspek kehidupan. Periode digital membuka peluang inovasi, efisiensi, dan pertumbuhan bisnis yang baru. Saat ini, pemanfaatan teknologi informasi dalam perusahaan telah menjadi kebutuhan penting yang mendukung berbagai aktivitas bisnis. Teknologi informasi berperan menjadikan data sebagai aset berharga bagi keberlanjutan bisnis, karena mampu membantu perusahaan dalam proses pengambilan keputusan, pengelolaan aset informasi, serta akses dan berbagi informasi dengan cepat, mudah, efektif, dan efisien[1]. Meskipun demikian, juga muncul tantangan baru mengenai keamanan siber, privasi data, dan perubahan yang terus-menerus[2]. Menurut Badan Siber dan Sandi Negara (BSSN) kemajuan teknologi yang cepat dan perubahan pola bisnis yang dinamis telah menghasilkan risiko keamanan informasi yang baru[3].

PT XYZ merupakan sebuah Software House yang merancang dan mengembangkan solusi perangkat lunak inovatif, memiliki fokus utama pada desain dan pengembangan aplikasi website, aplikasi seluler, dan *Progressive Web Apps (PWA)*[4]. Pada tahun 2021 PT XYZ mengalami suatu insiden berupa peretasan akun salah satu aplikasi marketing mereka yang memberi dampak kerugian bagi PT XYZ berupa pembatalan kerjasama dari beberapa perusahaan serta ganti rugi sebesar 15 juta rupiah. Selain itu PT XYZ juga telah mengalami kejahatan siber lainnya berupa *ransomeware* yang mengekripsi website pemasaran PT XYZ. Beberapa kejadian ini menjadi pertanda bahwa kurang matangnya persiapan keamanan siber di PT XYZ sehingga penelitian *Analisis Tingkat Kematangan Keamanan Siber di PT XYZ* akan membantu perusahaan tersebut untuk mengidentifikasi dengan lebih jelas kekuatan dan kelemahan pada setiap aspek keamanan siber yang perlu ditingkatkan.

Pentingnya informasi ini juga didukung oleh Undang-undang Perlindungan Data Pribadi (UU PDP) Nomor 27 Tahun 2022 yang bertujuan untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi dan menjamin hak konstitusional subjek data pribadi[5]. Kombinasi dari analisis kematangan keamanan siber dan adanya UU PDP ini akan memberikan arah yang lebih jelas menuju perlindungan data pribadi yang lebih baik dalam lingkungan teknologi yang terus berkembang di Indonesia.

Cyber Security Maturity (CSM) merupakan suatu alat ukur yang dirancang oleh Badan Siber dan Sandi Negara (BSSN) untuk menilai tingkat kematangan keamanan siber suatu organisasi. Dengan bantuan alat ini, PT XYZ dapat memahami tingkat kematangan keamanan siber mereka dengan mengidentifikasi area yang memerlukan perbaikan.

e-ISSN: 2548-6861

Tujuan utamanya adalah untuk meningkatkan keamanan siber di PT XYZ dan memungkinkan mereka menghadapi ancaman siber dengan lebih efisien. Hasil dari penelitian ini yaitu berupa skor kematangan keamanan siber beserta penjelasan mengenai kekuatan dan kelemahan PT XYZ agar bisa digunakan sebagai referensi untuk meningkatkan keamanan siber di PT XYZ.

A. *Tinjauan Pustaka*

1. Penelitian yang dilakukan oleh Delpia Amanda dkk pada tahun 2023 dengan judul "Analisis Tingkat Kematangan Keamanan Informasi Menggunakan NIST Cybersecurity Framework dan CMMI". Dalam penelitian ini, penulis mengevaluasi tingkat keamanan informasi pada SIAKAD Untan dengan menggunakan NIST CSF sebagai panduan dalam manajemen risiko untuk meningkatkan keamanan siber[6], serta memanfaatkan CMMI sebagai model pendekatan untuk menilai kematangan dan kapabilitas perangkat lunak[7].
2. Penelitian yang dilakukan oleh Rusyadi Umar dkk pada tahun 2019 dengan judul "Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI)". Dalam penelitian ini, penulis menganalisis keamanan administrasi sistem informasi pada BISKOM UAD Yogyakarta menggunakan COBIT 5 yang berfungsi sebagai panduan standar praktik manajemen teknologi informasi, serta CMMI yang digunakan untuk mencapai standar tingkat pencapaian[7].
3. Penelitan yang dilakukan oleh Irwan Suryono pada tahun 2023 yang berjudul "Evaluasi Penilaian Mandiri Penerapan SMKI di Salah Satu Lingkungan K/L". Dalam penelitian ini, penulis mengevaluasi penerpan SMKI (Sistem Manajemen Keamanan Informasi) di salah satu lingkungan kementrian/lembaga menggunakan Cyber Security Maturity (CSM) yang digunakan untuk mengidentifikasi kesenjangan antara kondisi pengelolaan keamanan siber saat ini dan kondisi ideal (yang diharapkan). Selain itu, penulis juga menggunakan Indeks KAMI sebagai alat untuk memberikan gambaran kepada pimpinan instansi/perusahaan mengenai kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi[8].
4. Penelitian yang dilakukan oleh Mohammad Afdhal Jauhari dkk pada tahun 2024 yang berjudul "Pengukuran Kematangan Keamanan Siber pada Perusahaan Teknologi Informasi dengan Framework Center for Internet Security Controls". Dalam hal ini penulis menggunakan CIS Controls yang dianggap lebih bersifat teknis dan fleksibel serta menekankan pentingnya penerapan *host-based firewall* untuk mengurangi risiko *ransomeware*[9].

Judul Penelitian	**Metode**	**Hasil Penelitian**
Analisis Tingkat Kematangan Keamanan Informasi Menggunakan NIST Cybersecurity Framework dan CMMI	NIST Cybersecurity Framework dan CMMI	Nilai maturity level dari SIAKAD Untan di UPT TIK berada pada level 2 dengan total skor kematangan 1.83.
Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI)	COBIT 5 dan CMMI	Nilai maturity level pada instansi ABC berada pada Level 4 dengan total skor indeks kematangan 4.458.
Evaluasi Penilaian Mandiri Penerapan SMKI di Salah Satu Lingkungan K/L	Cyber Security Maturity (CSM) dan Indeks KAMI	Nilai maturity level pada penelitian ini berada pada Level 4 dengan total skor indeks kematangan 3.62.
Pengukuran Kematangan Keamanan Siber pada Perusahaan Teknologi Informasi	CIS Controls	Nilai maturity keamanan siber pada penelitian ini menujukkan skor 0.41.

dengan Framework Center for Internet Security Controls		

B. *Cyber Security Maturity (CSM)*

Cyber Security Maturity (CSM) merupakan suatu alat yang telah dikembangkan oleh Badan Siber Sandi Negara (BSSN) yang dapat digunakan untuk menilai tingkat kematangan keamanan siber dalam suatu organisasi. Hasil penilaian ini mencakup skor atau nilai yang menunjukkan tingkat kematangan keamanan siber dari level 1 (implementasi awal) hingga level 5 (implementasi optimal). Indeks Maturity Level yang terdapat dalam CSM disajikan pada *Tabel 1.1*[10].

Maturity Level	**Rentang Nilai**
Level 1 (Implementasi Awal)	0.00-1.50
Level 2 (Implementasi Berulang)	1.51-2.50
Level 3 (Implementasi Terdefenisi)	2.51-3.50
Level 4 (Implementasi Terkelola)	3.51-4.50
Level 5 (Implementasi Optimal)	4.51-5.00

Tabel 1. 1 Indeks Maturity Level

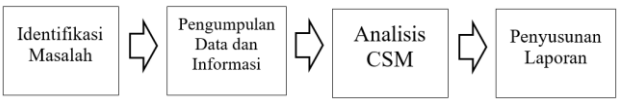
Adapun deskripsi dari masing-masing level disajikan pada *Tabel 1.2*.

Level	**Ciri-ciri**	**Deskripsi**	**Warna**
Level 1 (Implementasi Awal)	- Tidak terukur - Tidak konsisten - Risiko siber tinggi	Penerapan keamanan siber tidak dapat terukur dengan baik, risiko siber sangat tinggi	Merah (M)
Level 2 (Implementasi Berulang)	- Terorganisir - Tidak konsisten - Berulang	Penerapan keamanan siber sudah terorganisir, tetapi belum dapat terukur dengan baik, risiko siber tinggi.	Oren (O)
Level 3 (Implementasi Terdefenisi)	- Terorganisir - Konsisten - Riviu Berkala	Penerapan keamanan siber mulai dapat terukur dengan baik.	Kuning (K)
Level 4 (Implementasi Terkelola)	- Terorganisir - Riviu Berkala - Berkelanjutan	Penerapan keamanan siber dapat terukur dengan baik	Hijau Muda (HM)
Level 5 (Implementasi Optimal)	- Otomatisasi - Terintegrasi - Membudaya	Penerapan keamanan siber dapat terukur dengan sangat baik, keamanan siber menjadi budaya organisasi	Hijau Tua (HT)

Tabel 1. 2 Indeks Maturity Level dan Representasi Warna

II. METODE

Metode penelitian yang digunakan adalah sebagai berikut:



A. *Identifikasi Masalah*

Metode penelitian dimulai dengan mengidentifikasi masalah keamanan siber yang terjadi di PT XYZ berupa peretasan akun dan *ransomeware* yang menyebabkan PT XYZ mengalami kerugian. Identifikasi masalah ini dilakukan melalui sesi wawancara.

B. *Pengumpulan Data dan Informasi*

Hal ini melibatkan pengumpulan beragam sumber informasi, termasuk literatur ilmiah, dokumen terkait organisasi, dan juga wawancara. Dimulai dengan pemilihan responden berdasarkan peran dan tanggungjawab responden di PT XYZ. Selanjutnya melakukan wawancara menggunakan daftar pertanyaan yang sudah tersedia di *CSM Tools*. Jawaban yang didapatkan dari narasumber perlu diverifikasi dengan bukti untuk memastikan jawaban tersebut valid dan dapat dipercaya.

C. *Analisis CSM*

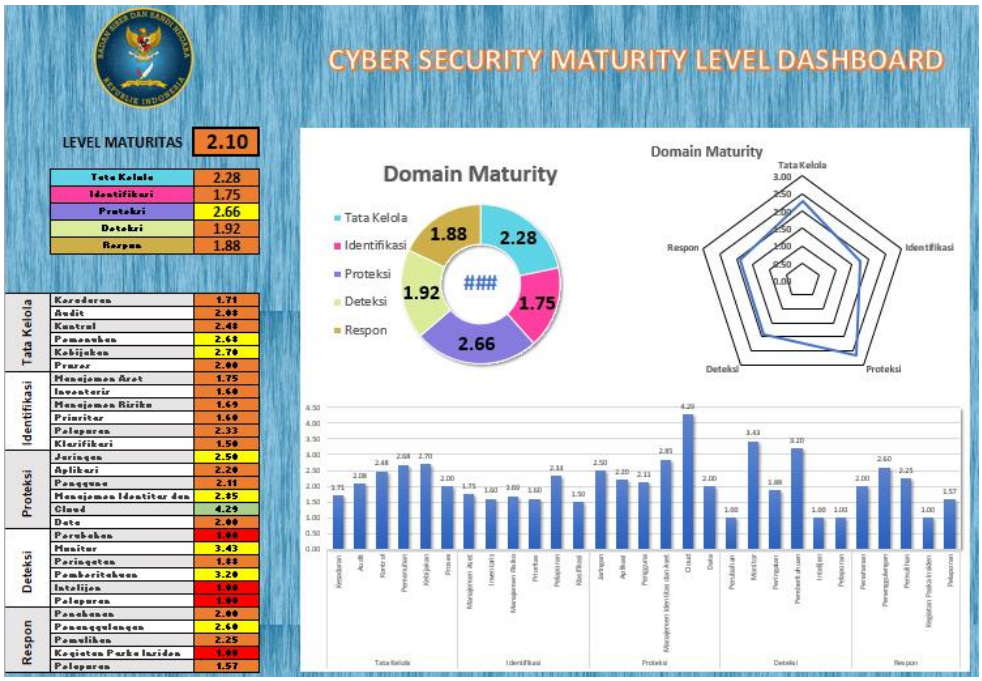
Analisis CSM ini melibatkan penggunan CSM *Tools* yang akan menghitung indeks kematangan dan level kematangan serta menyediakan visualisasi data berupa grafik radar. *CSM Tools* sudah dilengkapi formula yang secara otomatis menghitung skor berdasarkan jawaban yang dipilih dari *dropdown*. Jawaban yang telah diverifikasi kemudian dimasukkan ke dalam *CSM Tools* dan *tools* akan secara otomatis menganalisis data tersebut dan memberikan hasil dalam bentuk skor untuk setiap aspek yang dinilai.

D. *Penyusunan Laporan*

Penyusunan laporan ini mencakup semua temuan dari tahapan identifikasi masalah, pengumpulan data, dan hasil analisis CSM.

III. HASIL DAN PEMBAHASAN

Hasil pembahasan dari penelitian ini menunjukkan bahwa PT XYZ berada di level 2 dengan skor kematangan 2.10. Visualisasi data ditunjukkan pada gambar 3.1.



Gambar 3. 1Maturity Level PT XYZ

Tata Kelola		Identifikasi		Proteksi		Deteksi		Respon	
2.28		1.75		2.66		1.92		1.88	
Kesadaran	1.71	Manajemen Aset	1.75	Jaringan	2.50	Perubahan	1.00	Penahanan	2.00
Audit	2.08	Inventaris	1.60	Aplikasi	2.20	Monitor	3.43	Penanggulangan	2.60
Kontrol	2.48	Manajemen Risiko	1.69	Pengguna	2.11	Peringatan	1.88	Pemulihan	2.25
Pemenuhan	2.68	Prioritas	1.60	Manajemen Identitas dan	2.85	Pemberitahuan	3.20	Kegiatan Paska	1.00
Kebijakan	2.70	Pelaporan	2.33	Cloud	4.29	Intelijen	1.00	Pelaporan	1.57
Proses	2.00	Klasifikasi	1.50	Data	2.00	Pelaporan	1.00		

Gambar 3. 2 Skor Maturity PT XYZ

A. Distribusi Pertanyaan Setiap Aspek

Adapun pada Tabel 3.1 hingga Tabel 3.5 di bawah ini menyajikan jumlah pertanyaan yang mendapatkan skor tertentu untuk setiap sub aspek dalam aspek tata kelola, identifikasi, proteksi, deteksi, dan juga respon.

a. Total Skor Sub Aspek

$$Total\ Skor\ Sub\ Aspek = (n1\ x\ 1.00) + (n2\ x\ 2.00) + (n3\ x\ 3.00) + (n4\ x\ 4.00) + (n5\ x\ 5.00)$$

b. Skor Rata-rata

$$Skor\ Rata - rata = \frac{Total\ Skor\ Sub\ Aspek}{Jumlah\ Pertanyaan}$$

c. Total Skor Aspek

$$Total\ Skor\ Aspek = \frac{Jumlah\ Skor\ Rata - rata}{Jumlah\ Sub\ Aspek}$$

Tata Kelola	Banyak Pertanyaan Berdasarkan Skor (n)					Total Skor Sub Aspek	Jumlah Pertanyaan	Skor rata-rata
	1.00	2.00	3.00	4.00	5.00			
Kesadaran	10	4	2	-	1	29	17	1.71
Audit	6	2	1	3	-	25	12	2.08
Kontrol	9	6	1	2	5	57	23	2.48
Pemenuhan	5	6	1	4	3	51	19	2.68
Kebijakan	2	4	1	1	2	27	10	2.70
Proses	7	3	2	1	1	28	14	2.00
Total Skor Aspek								**2.28**

Tabel 3. 1 Distribusi Pertanyaan Aspek Tata Kelola

Identifikasi	Banyak Pertanyaan Berdasarkan Skor (n)					Total Skor Sub Aspek	Jumlah Pertanyaan	Skor rata-rata
	1.00	2.00	3.00	4.00	5.00			
Manajemen Aset	3	-	-	1	-	7	4	1.75
Inventaris	4	-	-	1	-	8	5	1.60
Manajemen Risiko	8	3	1	-	1	22	13	1.69
Prioritas	4	-	-	1	-	8	5	1.60
Pelaporan	2	-	-	-	1	7	3	2.33
Klasifikasi	3	-	1	-	-	6	4	1.50
Total Skor Aspek								**1.75**

Tabel 3. 2 Distribusi Pertanyaan Aspek Identifikasi

Proteksi	Banyak Pertanyaan Berdasarkan Skor (n)					Total Skor Sub Aspek	Jumlah Pertanyaan	Skor rata-rata
	1.00	2.00	3.00	4.00	5.00			
Jaringan	2	5	5	2	-	35	14	2.50
Aplikasi	-	8	2	-	-	22	10	2.20
Pengguna	6	-	1	-	2	19	9	2.11
Manajemen Identitas dan Aset	4	2	3	-	4	37	13	2.85
Cloud	-	1	-	2	4	30	7	2.29
Data	5	-	-	1	1	14	7	2.00
Total Skor Aspek								**2.66**

Tabel 3. 3 Distribusi Pertanyaan Aspek Proteksi

e-ISSN: 2548-6861

Deteksi	Banyak Pertanyaan Berdasarkan Skor (n)					Total Skor Sub Aspek	Jumlah Pertanyaan	Skor rata-rata
	1.00	2.00	3.00	4.00	5.00			
Perubahan	3	-	-	-	-	3	3	1.00
Monitor	2	4	-	2	6	48	14	3.43
Peringatan	4	2	1	1	-	15	8	1.88
Pemberitahuan	1	1	-	2	1	16	5	3.20
Intelejen	11	-	-	-	-	11	11	1.00
Pelaporan	5	-	-	-	-	5	5	1.00
Total Skor Aspek								**1.92**

Tabel 3. 4 Distribusi Pertanyaan Aspek Deteksi

Respon	Banyak Pertanyaan Berdasarkan Skor (n)					Total Skor Sub Aspek	Jumlah Pertanyaan	Skor rata-rata
	1.00	2.00	3.00	4.00	5.00			
Penahanan	9	-	-	-	3	24	12	2.00
Penanggulangan	1	2	1	-	1	13	5	2.60
Pemulihan	2	-	1	1	-	9	4	2.25
Kegiatan Paska Insiden	4	-	-	-	-	4	4	1.00
Pelaporan	3	4	-	-	-	11	7	1.57
Total Skor Aspek								**1.88**

Tabel 3. 5 Distribusi Pertanyaan Aspek Respon

Aspek	**Rata-rata Total Skor Aspek**
Tata Kelola	2.28
Identifikasi	1.75
Proteksi	2.66
Deteksi	1.92
Respon	1.88
Total Skor Indeks	**2.10**

Tabel 3. 6 Total Skor Indeks

IV. KESIMPULAN

A. Aspek Tata Kelola

Aspek tata kelola pada PT XYZ memperoleh skor kematangan 2.28. Penilaian ini didasarkan pada:

Warna	Jumlah Sub Aspek	Sub Aspek
Oren (O)	4	Kesadaran, Audit, Kontrol, Proses
Kuning (K)	2	Pemenuhan, Kebijakan

Tabel 4. 1Klasifikasi Warna Aspek Tata Kelola

a. Sub Aspek Kesadaran

Kekuatan:

1. Sebagian karyawan memahami dan menerapkan kebijakan informasi di lingkungan kerja PT XYZ.
2. Sebagian karyawan memberikan kontribusi terhadap efektivitas sistem manajemen keamanan informasi.

Kekurangan:

1. Tidak dilakukannya pelatihan berkala tentang keamanan informasi secara terjadwal di PT XYZ.
2. Tidak adanya praktik dalam manajemen kerentanan siber dan mitigasi di PT XYZ.
3. Tidak adanya simulasi phishing dan pelatihan secure coding di PT XYZ.
4. Tidak ada komunikasi kepada stakeholder tentang kerentanan siber di PT XYZ.

b. Sub Aspek Audit

Kekuatan:

1. PT XYZ telah melakukan pemeriksaan latar belakang untuk karyawan baru.
2. PT XYZ telah melakukan reviu izin akses akun pengguna setiap tiga bulan.

Kekurangan:

1. Tidak ada reviu berkala untuk kebijakan perlindungan data pribadi di PT XYZ.
2. Tidak ada reviu untuk algoritma enkripsi dan evaluasi risiko di PT XYZ.
3. Tidak ada implementasi vulnerability scanning atau penetration testing yang terkoordinasi di PT XYZ.
4. Tidak ada reviu internal keamanan informasi berkala di PT XYZ.
5. Dokumentasi yang tidak lengkap untuk standar konfigurasi dan aliran data di PT XYZ.

c. Sub Aspek Kontrol

Kekuatan:

1. PT XYZ telah menggunakan firewall dan perlindungan end user.
2. PT XYZ telah menggunakan antivirus dan antimalware yang terpusat.
3. PT XYZ telah melakukan filterisasi file lampiran email.

Kekurangan:

1. PT XYZ tidak pernah melakukan penerapan dan reviu kontrol keamanan.
2. PT XYZ tidak pernah melakukan penerapan metode sandboxing terhadap lampiran email.
3. Tidak ada implementasi DMARC atau protokol otentikasi email di PT XYZ.
4. Tidak ada penerapan risk assessment dan continual improvement di PT XYZ.

d. Sub Aspek Pemenuhan

Kekuatan:

1. PT XYZ telah menerapkan prosedur untuk memastikan kepatuhan terhadap perundang-undangan dan persyaratan kontrak yang berhubungan dengan hak kekayaan intelektual serta penggunaan produk perangkat lunak proprietary.
2. PT XYZ telah melakukan perlindungan dan pemeliharaan dokumen agar tidak hilang, hancur, dipalsukan, atau diakses oleh pihak yang tidak sah sesuai dengan persyaratan perundang-undangan, peraturan, dan kontrak yang berlaku.

Kekurangan:

1. PT XYZ tidak memiliki kebijakan atau prosedur yang terdokumentasi mengenai pemberitahuan jika terjadi pelanggaran terhadap data pribadi.
2. Tidak ada Business Continuity Plan (BCP) dan Disaster Recovery Plan (DRP) untuk data pribadi.
3. PT XYZ tidak melakukan verifikasi praktik secure coding.
4. PT XYZ tidak memiliki batasan penyimpanan data yang dimonitor (retensi data).

e. Sub Aspek Kebijakan

Kekuatan:

1. PT XYZ telah menerapkan kebijakan sanksi untuk karyawan yang tidak patuh.
2. PT XYZ telah menerapkan kebijakan single ID dan otorisasi.

Kekurangan:

e-ISSN: 2548-6861

1. PT XYZ tidak memiliki kebijakan terminasi dengan masa tenggang.
2. PT XYZ tidak menetapkan proses untuk menerima dan menangani laporan kerentanan software, serta tidak menyediakan sarana bagi entitas eksternal untuk menghubungi bagian keamanan organisasi.
3. PT XYZ tidak memiliki kebijakan untuk laporan kehilangan perangkat.
4. PT XYZ tidak memiliki kebijakan metode penghapusan data.

f. Sub Aspek Proses

Kekuatan:

1. PT XYZ telah melakukan konfigurasi startup switch dan router selalu disinkronkan dengan running configs, yang menunjukkan upaya untuk menjaga konsistensi dan keamanan konfigurasi jaringan.
2. Terdapat prosedur untuk menambah/mengubah/menghapus hak akses ketika terjadi perpindahan karyawan, termasuk otorisasi dan persetujuan.

Kekurangan:

1. Kebijakan dan prosedur keamanan informasi tidak dikembangkan sesuai dengan kerangka kerja dan standar yang diakui seperti ISO 27001, PCI-DSS, HIPAA, NIST, CIS, SANS, dll.
2. Kurangnya pengujian keamanan dan threat hunting secara berkala di PT XYZ.
3. Kurangnya proses formal untuk manajemen perubahan konfigurasi jaringan.

B. Aspek Identifikasi

Aspek Identifikasi pada PT XYZ memperoleh skor kematangan 1.79. Penilaian ini didasarkan pada:

Warna	Jumlah Sub Aspek	Sub Aspek
Oren (O)	6	Manajemen Aset, Inventaris, Manajemen Risiko, Prioritas, Pelaporan, Klasifikasi

Tabel 4. 2 Klasifikasi Warna Aspek Identifikasi

a. Sub Aspek Manajemen Aset

Kekuatan:

1. PT XYZ telah menggunakan alat manajemen konfigurasi sistem untuk otomatisasi konfigurasi perangkat keras dan lunak, menjaga konsistensi dan keamanan konfigurasi.

Kekurangan:

1. PT XYZ tidak melakukan perencanaan kapasitas secara berkala, berpotensi tidak memenuhi kebutuhan dan meningkatkan risiko keamanan.
2. PT XYZ tidak menerapkan patch keamanan pada perangkat keras dan lunak, membuat sistem rentan terhadap eksploitasi.

b. Sub Aspek Inventarisasi

Kekuatan:

1. IPT XYZ telah mengidentifikasi dan membatasi akses perangkat yang tidak diizinkan dengan respons cepat (maksimal 24 jam) setelah terdeteksi.

Kekurangan:

1. PT XYZ tidak melakukan inventarisasi data pada perangkat keras dan lunak.
2. PT XYZ tidak melakukan klasifikasi kritikalitas aset dan penetapan penanggung jawab untuk setiap aset, mengurangi pemahaman tentang nilai dan prioritas aset.
3. Organisasi tidak melakukan klasifikasi informasi (rahasia, terbatas, umum) yang menyebabkan ketidakjelasan tentang sensitivitas dan pentingnya informasi yang disimpan dan diproses.

c. Sub Aspek Manajemen Risiko

Kekuatan:

1. PT XYZ memiliki kebijakan membatasi penggunaan aset pihak ketiga pada jaringan, sehingga dapat mengendalikan risiko terkait akses pihak ketiga.
2. PT XYZ menyimpan data otentikasi di perangkat browser end user, sehingga memudahkan akses pengguna.

Kekurangan:

1. PT XYZ tidak melakukan analisis keterkaitan antara keamanan dan kenyamanan penggunaan aset, mengurangi pemahaman tentang dampaknya terhadap keamanan informasi.
2. PT XYZ tidak memiliki kebijakan dan implementasi yang jelas mengenai retensi data sensitif sehingga meningkatkan risiko retensi data yang tidak terkendali.
3. PT XYZ tidak melakukan pemeringkatan pada kerentanan yang teridentifikasi, yang mengakibatkan kurangnya prioritasi dalam penanganan kerentanan yang ada.
4. PT XYZ tidak memiliki risk register terdokumentasi untuk aplikasi yang memproses

data stakeholder/klien/konsumen/pelanggan, menghambat identifikasi, pemantauan, dan mitigasi risiko.

d. Sub Aspek Prioritas

Kekuatan:

1. Memprioritaskan aspek keamanan dalam beberapa pengambilan keputusan TI, menunjukkan kesadaran akan pentingnya keamanan dalam strategi TI.

Kekurangan:

1. PT XYZ tidak memperbaharui roadmap keamanan TI secara berkala.
2. PT XYZ tidak memiliki Business Impact Analysis (BIA) dan prioritasi upaya remediasi berdasarkan risiko.
3. PT XYZ tidak melakukan prioritasi langkah proteksi keamanan siber sehingga mengurangi fokus pada perlindungan terhadap serangan yang berpotensi merugikan organisasi.

e. Sub Aspek Pelaporan

Kekuatan:

1. PT XYZ mempertimbangkan kapasitas server dan perangkat jaringan dalam aspek keamanan.

Kekurangan:

1. PT XYZ tidak melakukan pengelolaan data log keamanan informasi sehingga mengurangi transparansi dan auditabilitas terhadap kejadian keamanan.
2. PT XYZ tidak menyusun profil keamanan informasi yang mencakup prioritas kerentanan dan rencana mitigasi.

f. Sub Aspek Klasifikasi

Kekuatan:

1. PT XYZ memiliki kebijakan untuk klasifikasi data yang menunjukkan kesadaran akan pentingnya mengelola dan melindungi data sesuai tingkat sensitivitas.

Kekurangan:

1. PT XYZ tidak memiliki metode atau standar untuk klasifikasi aset TI.
2. PT XYZ tidak pernah melakukan klasifikasi terhadap cyber threats.
3. PT XYZ tidak melakukan segmentasi jaringan berdasarkan fungsionalitas sehingga meningkatkan risiko karena tidak adanya pembatasan akses yang tepat di seluruh jaringan.

C. Aspek Proteksi

Aspek Proteksi pada PT XYZ memperoleh skor kematangan 2.66. Penilaian ini didasarkan pada:

Warna	Jumlah Sub Aspek	Sub Aspek
Oren (O)	3	Aplikasi, Pengguna, Data
Kuning (K)	2	Jaringan, Manajemen Identitas dan Aset
Hijau Muda	1	Cloud

Tabel 4. 3 Klasifikasi Warna Aspek Proteksi

a. Sub Aspek Jaringan

Kekuatan:

1. PT XYZ telah mengimplementasi Intrusion Prevention System (IPS) yang terkonfigurasi dan diperbarui.
2. PT XYZ telah mengkonfigurasi akses nirkabel dengan enkripsi.

Kekurangan:

1. PT XYZ tidak memiliki pengaturan spesifik untuk inbound dan outbound network traffic.
2. PT XYZ tidak memiliki filter malware untuk inbound network traffic.
3. Beberapa pengendalian keamanan jaringan, seperti port access control dan firewall filtering, belum diterapkan.
4. Beberapa fitur keamanan wireless, seperti pembatasan penggunaan wireless pada perangkat, belum diterapkan.
5. Tidak ada layanan filter DNS.

b. Sub Aspek Aplikasi

Kekuatan:

1. PT XYZ telah mengimplementasi pengecekan otomatis terhadap spam, phishing, dan malware pada sistem email.
2. PT XYZ menyimpanan master images pada server yang dikonfigurasi secara aman.

Kekurangan:

1. PT XYZ tidak membatasi aplikasi yang diunduh, diinstal, dan dioperasikan.
2. PT XYZ tidak memiliki pengelolaan patch pada aplikasi.
3. Tidak ada whitelist aplikasi untuk memastikan hanya software library yang authorized yang dapat dijalankan.
4. Tidak ada pembatasan penggunaan scripting tools.

c. Sub Aspek Pengguna

Kekuatan:

e-ISSN: 2548-6861

1. PT XYZ telah menggunakan antivirus pada semua perangkat endpoint.
2. PT XYZ telah mengatur penguncian perangkat setelah ketidakaktifan.
3. Tidak mengizinkan fitur auto-run content pada perangkat portable.
4. Pembatasan akses perangkat USB atau media penyimpanan eksternal.

Kekurangan:

1. PT XYZ tidak menggunakan Next Generation Endpoint Protection.
2. PT XYZ tidak mengimplementasikan web URL filtering, device control, dan application control.
3. PT XYZ tidak melakukan enkripsi pada perangkat mobile.
4. PT XYZ tidak menerapkan enkripsi pada media penyimpanan eksternal.

d. Sub Aspek Manajemen Identitas dan Akses

Kekuatan:

1. PT XYZ telah melakukan penggunaan password kompleks dan penggantian secara berkala.
2. PT XYZ menerapkan metode otentikasi melalui saluran terenkripsi untuk login jaringan.
3. PT XYZ memiliki pengaturan hak akses data.

Kekurangan:

1. PT XYZ tidak menggunakan Multi-Factor Authentication (MFA) untuk semua akses jaringan dan data sensitif.
2. PT XYZ tidak menerapkan OTP untuk transaksi berisiko tinggi.
3. PT XYZ tidak dapat melacak dan mendeteksi perilaku anomali transaksi.
4. Penggunaan metode otentikasi terenkripsi hanya untuk login jaringan, tidak untuk login aplikasi.

e. Sub Aspek Cloud

Kekuatan:

1. PT XYZ menggunakan Authorized Cloud Storage.
2. PT XYZ telah mengimplementasi Single Sign-On (SSO).
3. PT XYZ telah membatasi akses traffic cloud hanya dari alamat IP yang dikenal.
4. Penerapan Multi-Factor Authentication (MFA) oleh penyedia cloud.
5. Redundansi data center yang terpisah secara geografis.
6. Tidak dapat mengakses SSO melalui SSL VPN Tunnel.

Kekurangan:

1. Tidak membatasi traffic cloud hanya untuk kebutuhan bisnis.

f. Sub Aspek Data

Kekuatan:

1. PT XYZ telah melakukan backup berkala dan otomatis untuk semua data penting.
2. PT XYZ menyimpanan log setidaknya selama satu tahun.

Kekurangan:

1. PT XYZ tidak pernah melakukan pengujian data integrity.
2. PT XYZ tidak mengenkripsi untuk data stakeholder/klien/konsumen/pelanggan.
3. Tidak ada sinkronisasi otomatis untuk critical system clocks.

D. Aspek Deteksi

Aspek Deteksi pada PT XYZ memperoleh skor kematangan 1.92. Penilaian ini didasarkan pada:

Warna	Jumlah Sub Aspek	Sub Aspek
Merah (M)	3	Perubahan, Intelejen, Pelaporan
Oren (O)	1	Peringatan
Kuning (K)	2	Monitor, Pemberitahuan

Tabel 4. 4 Klasifikasi Warna Aspek Deteksi

a. Sub Aspek Perubahan

Kekurangan:

1. PT XYZ tidak memiliki Change Advisory Board (CAB) untuk meninjau dan menyetujui perubahan konfigurasi, yang bisa menyebabkan perubahan tak terkendali dan downtime.
2. PT XYZ tidak memiliki proses manajemen perubahan yang sistematis, sehingga sulit melacak dan mengelola perubahan yang dilakukan.
3. Perubahan konfigurasi pada peralatan jaringan tidak terdeteksi secara otomatis sehingga mengurangi visibilitas terhadap perubahan yang mempengaruhi keamanan dan performa jaringan.

b. Sub Aspek Monitoring

Kekuatan:

1. PT XYZ sudah menerapkan monitoring (pemantauan dan notifikasi) terhadap aktivitas lalu lintas jaringan secara otomatis.

2. PT XYZ telah menerapkan mekanisme dan monitoring dan deteksi penggunaan enkripsi yang tidak sah.
3. PT XYZ telah menerapkan monitoring log perangkat keamanan, jaringan, dan aplikasi.
4. PT XYZ telah melakukan monitoring akses pengguna dan infrastruktur.
5. PT XYZ telah melakukan deteksi otomatis Wireless Access Point yang terhubung ke jaringan LAN.
6. PT XYZ telah mengalokasi kapasitas penyimpanan log sesuai kebutuhan.

Kekurangan:

1. PT XYZ tidak menerapkan monitoring terhadap akses dan perubahan pada data sensitif seperti File Integrity Monitoring atau Event Monitoring.
2. PT XYZ tidak memiliki sistem pencegahan kehilangan data sensitif (DLP).
3. Tidak ada pelatihan keterampilan untuk tim monitoring di PT XYZ.
4. Tidak ada monitoring aktivitas pihak ketiga untuk deteksi keamanan siber di PT XYZ.

c. Sub Aspek Peringatan

Kekuatan:

1. PT XYZ telah melakukan mekanisme deteksi akses tidak diizinkan secara otomatis.
2. PT XYZ telah mendeteksi kegagalan login akun admin pada perangkat jaringan, server, dan aplikasi.

Kekurangan:

1. PT XYZ tidak memiliki perangkat anti-malware untuk scanning otomatis terhadap removable media.
2. PT XYZ tidak menerapkan automated port scan berkala dan alert untuk port tidak sah.
3. PT XYZ tidak memiliki ticketing system untuk melacak progres events post-notification.
4. Organisasi tidak pernah melakukan escalation profile untuk setiap security event yang ditemukan.

d. Sub Aspek Pemberitahuan

Kekuatan:

1. PT XYZ menyimpanan log URL yang diakses oleh karyawan.
2. PT XYZ dapat mendeteksi aktivitas anomali login secara otomatis.

Kekurangan:

1. PT XYZ tidak menerapkan SOC atau manajemen teknis 24x7 untuk menangani insiden prioritas tinggi.
2. PT XYZ tidak menerapkan event notification yang berbeda untuk setiap jenis eskalasi berdasarkan prioritas.

e. Sub Aspek Intelejen

Kekuatan:

1. PT XYZ memiliki pemahaman terhadap Indicator of Compromise (IOC) dari serangan siber.

Kekurangan:

1. PT XYZ tidak pernah memperoleh informasi dari multiple threat intelligence feeds.
2. PT XYZ hanya mengandalkan browsing melalui search engine untuk mendapatkan isu keamanan siber terkini.
3. PT XYZ tidak pernah melakukan vulnerability scanning.
4. PT XYZ tidak memiliki unit khusus untuk Cyber Threat Intelligence (CTI).

f. Sub Aspek Pelaporan

Kekurangan:

1. PT XYZ tidak memiliki jadwal untuk meninjau metrik security event secara sistematis.
2. PT XYZ tidak melakukan briefing kepada Top Level Management tentang kondisi keamanan siber.
3. PT XYZ tidak memiliki mekanisme sharing informasi hasil deteksi.

E. Aspek Respon

Aspek Deteksi pada PT XYZ memperoleh skor kematangan 1.88. Penilaian ini didasarkan pada:

Warna	Jumlah Sub Aspek	Sub Aspek
Merah (M)	1	Kegiatan Paska Insiden
Oren (O)	3	Penahanan, Pemulihan, Pelaporan
Kuning (K)	1	Penanggulangan

Tabel 4. 5 Klasifikasi Warna Aspek Respon

a. Sub Aspek Penahanan

Kekuatan:

1. PT XYZ memiliki standar operasional prosedur (SOP) dan formulir pelaporan penanganan insiden yang diketahui oleh pihak terkait.
2. Daftar kontak tim penanganan insiden internal dan eksternal diupdate sepenuhnya.

e-ISSN: 2548-6861

3. Organisasi melakukan backup data karyawan ke cloud organisasi.

Kekurangan:

1. PT XYZ tidak memiliki kebijakan penanganan insiden yang terkoordinasi dengan business continuity planning (BCP).
2. PT XYZ tidak pernah melakukan latihan untuk respon insiden.
3. Waktu diskoneksi segmen jaringan terlalu lama saat terjadi infeksi malware.
4. PT XYZ tidak memiliki sumber daya redundan untuk sistem penting dalam situasi darurat.
5. PT XYZ tidak memiliki metode terdokumentasi untuk melaporkan penyalahgunaan informasi kepada stakeholder.

b. Sub Aspek Penanggulangan

Kekurangan:

1. PT XYZ tidak memiliki peralatan sumber daya analisis seperti daftar host, analisis protokol, dokumentasi protokol keamanan, diagram jaringan, daftar aset penting, alat digital forensic, dan lain sebagainya.
2. PT XYZ hanya mampu mendeteksi insiden tanpa kemampuan melakukan analisis mendalam dan memberikan rekomendasi solusi.
3. PT XYZ tidak memiliki sumber daya redudan untuk sistem penting/kritikal yang dapat digunakan segera jika sistem utama down.
4. PT XYZ tidak melakukan scanning ulang untuk memastikan kerentanan telah ditutup setelah patching.
5. PT XYZ tidak memiliki metode terdokumentasi dan diinformasikan kepada stakeholder, klien, konsumen, atau pelanggan untuk melaporkan penyalahgunaan informasi.

c. Sub Aspek Pemulihan

Kekurangan:

1. Tim respon insiden tidak cepat mendapat bantuan dari tim manajemen krisis.
2. PT XYZ tidak memiliki pencatatan langkah penanggulangan insiden dengan format baku.
3. PT XYZ memiliki keterbatasan memastikan ketersediaan server cadangan dalam waktu kurang dari 3 jam.
4. Waktu restore data dari backup melebihi Recovery Point Objective (RPO) yang ditetapkan.

d. Sub Aspek Kegiatan Paska Insiden

Kekurangan:

1. PT XYZ tidak melakukan review root cause insiden.
2. PT XYZ tidak melakukan review laporan insiden yang pernah terjadi.
3. Hasil review insiden tidak dilaporkan kepada top management dan pemangku kepentingan.
4. PT XYZ tidak memastikan pencapaian Service Level Agreement (SLA) dalam penanganan insiden.

e. Sub Aspek Pelaporan

Kekurangan:

1. PT XYZ tidak memiliki metrik perhitungan biaya dan ROI untuk keamanan siber.
2. PT XYZ tidak menggunakan sumber referensi terpercaya untuk perhitungan biaya insiden.
3. PT XYZ tidak memiliki mekanisme pelaporan anomali dan insiden secara terbuka.
4. PT XYZ tidak merancang standar waktu dan mekanisme pelaporan yang jelas.

Dengan demikian, dapat disimpulkan bahwa penerapan keamanan siber di PT XYZ telah memiliki proses yang sudah terorganisir namun masih bersifat informal, dilakukan secara berulang namun belum konsisten, serta belum dilakukan secara berkelanjutan. Oleh karena itu, penerapan keamanan siber pada level ini tidak dapat terukur dengan baik dan organisasi memiliki tingkat risiko siber yang tinggi.

V. DAFTAR PUSTAKA

[1] B. S. Deva and R. Jayadi, "Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro," *JATI*, vol. 12, no. 2, pp. 106–117, Sep. 2022, doi: 10.34010/jati.v12i2.6829.

[2] Z. Kurniawan, "Daya Saing Sumber Daya Manusia di Era Digitalisasi," *EBI*, vol. 5, no. 2, pp. 83–88, Sep. 2023, doi: 10.52061/ebi.v5i2.182.

[3] R. Adi Putra Pratama Gala, R. Sengkey, and C. Punusingon, "Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI," *Jurnal Teknik Informatika*, vol. 15 no 3, pp. 189–198, Sep. 2020.

[4] "Media Sarana Digital." Accessed: Nov. 12, 2023. [Online]. Available: https://mediasaranadigitalindo.com

[5] "Salinan UU Nomor 27 Tahun 2022."

[6] T. Tan and B. Soewito, "Manajemen Risiko Serangan Siber Menggunakan Framework NIST CYBERSECURITY di Universitas ZXC," vol. 6, 2022.

[7] R. Umar, I. Riadi, and E. Handoyo, "Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration

(CMMI)," *J. Sistem Info. Bisnis*, vol. 9, no. 1, p. 47, May 2019, doi: 10.21456/vol9iss1pp47-54.
[8] M. A. Adiguna, "Evaluasi Penilaian Mandiri Penerapan SMKI di Salah Satu Lingkungan K/L," Mar. 2023, doi: 10.5281/ZENODO.7720440.
[9] M. A. Jauhari, B. A. Wardijono, and E. Hegarini, "Pengukuran Kematangan Keamanan Siber pada Perusahaan Teknologi Informasi dengan Framework Center for Internet Security Controls," *saintekom*, vol. 14, no. 1, pp. 72–83, Mar. 2024, doi: 10.33020/saintekom.v14i1.610.
[10] D. Amanda, N. Mutiah, and S. Ramayudha, "Analisis Tingkat Kematangan Keamanan Informasi Menggunakan NIST Cybersecurity Framework dan CMMI," *Jurnal Komputer dan Aplikasi*, vol. 11, 2023.