SAIN TEKOM
ISSN 2088-1770 (Print)
ISSN 2503-3247(Online)
Vol. 14 No.1 (2024) 72-83

JURNAL
SAINTEKOM
Sains, Teknologi, Komputer, dan Manajemen

Pengukuran Kematangan Keamanan Siber pada Perusahaan Teknologi Informasi dengan *Framework* Center for Internet Security Controls

*Mohammad Afdhal Jauhari[1], Bheta Agus Wardijono[2], Ega Hegarini [3]
[1)] Magister Teknologi Informasi, STMIK Jakarta STI&K
Jl. TB Simatupang No. 51B, Pasar Minggu, Jakarta Selatan, DKI Jakarta
[2)] Sistem Komputer STMIK Jakarta STI&K
Jl. BRI Radio Dalam No. 17, Kebayoran Baru, Jakarta Selatan, DKI Jakarta
[3)] Sistem Informasi, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Gunadarma
Jl. Margonda Raya No.100, Beiji, Depok, Jawa Barat
Email: [1]afdhaljauhari@gmail.com, [2]bhetaagus@gmail.com, [3]ega@staff.gunadarma.ac.id

ABSTRACT

This research evaluates the cybersecurity maturity of a technology information company in Jakarta, using the CIS Controls framework that encompasses all controls within Implementation Group 1 (IG1). The company has not conducted formal measurements regarding cybersecurity maturity, leading to uncertainty about the effectiveness of security efforts. The aim of this study is to measure, assess, and provide recommendations to enhance cybersecurity within the company. The research methodology involves an assessment of CIS Controls implementation and maturity level measurements. The measurement results indicate a low level of maturity, with an overall score of 0.41. The company needs to make significant improvement efforts in the cybersecurity aspect. Recommendations derived from this analysis emphasize the need for policy enhancements, control improvements, and increased employee training, serving as a guide for the company to strengthen weak cybersecurity aspects. The company should adopt a sustainable approach with management commitment and active engagement of all stakeholders.

Keywords : cybersecurity; cybersecurity maturity; security policies; maturity measurement; security analysis

ABSTRAK

Penelitian ini mengevaluasi kematangan keamanan siber pada sebuah perusahaan teknologi informasi di Jakarta dengan menggunakan kerangka kerja CIS *Controls* yang mencakup seluruh kontrol dalam *Implementation Group 1 (IG1)*. Perusahaan belum pernah melakukan pengukuran formal terkait kematangan keamanan siber, yang menyebabkan ketidakjelasan mengenai efektivitas upaya keamanan. Tujuan penelitian ini adalah untuk mengukur, mengevaluasi dan menawarkan rekomendasi guna meningkatkan keamanan siber di perusahaan tersebut. Metodologi penelitian melibatkan penilaian implementasi CIS *Controls* serta pengukuran tingkat kematangan. Hasil pengukuran menunjukkan tingkat kematangan yang rendah, dengan skor keseluruhan sebesar 0,41. Perusahaan perlu melakukan upaya perbaikan secara signifikan dalam aspek keamanan siber. Rekomendasi yang diajukan berdasarkan analisis ini menekankan perlunya peningkatan kebijakan, perbaikan kontrol dan peningkatan pelatihan untuk karyawan, agar dapat menjadi panduan bagi perusahaan dalam memperkuat aspek keamanan siber yang masih lemah. Perusahaan perlu mengadopsi pendekatan berkelanjutan dengan keterlibatan manajemen dan partisipasi aktif dari semua pemangku kepentingan.

Kata kunci : keamanan siber; kematangan keamanan siber; kebijakan keamanan; pengukuran kematangan; analisis keamanan

Diterima Redaksi: 21-1-2024 | Selesai Revisi: 2-2-2024 | Diterbitkan Online: 31-3-2024

1. PENDAHULUAN

Era digital yang semakin berkembang pesat, keamanan siber menjadi salah satu aspek yang kritis bagi perusahaan. Penerapan keamanan siber di organisasi dapat mengurangi biaya yang harus dikeluarkan akibat adanya pelanggaran, menjaga kepatuhan peraturan dan mengurangi ancaman siber. Hal ini membantu organisasi melindungi reputasi bisnis, keuangan, operasi dan kepercayaan pelanggan dari serangan siber yang merugikan (Amazon Web Service, 2023).

Ketika sebuah perusahaan telah mencapai tingkat kompleksitas yang tinggi sebagaimana perusahaan TI, tantangan utama yang dihadapi adalah menjaga keamanan data dan sistem mereka. Salah satunya adalah perusahaan TI di Jakarta yang menjadi fokus dalam penelitian ini. Perusahaan ini menyediakan berbagai layanan TI, mulai dari konsultasi manajemen TI, pengembangan sistem informasi hingga pelatihan dan sertifikasi TI.

Perusahaan ini belum pernah melakukan pengukuran formal terkait kematangan keamanan siber, sehingga menyebabkan ketidakjelasan tentang sejauh mana efektivitas upaya keamanan yang telah dilakukan. Perusahaan ini pernah mengalami serangan siber serius dalam bentuk infeksi *ransomware* yang menyebabkan kerugian besar termasuk hilangnya dokumen-dokumen berharga. *Ransomware* adalah jenis *malware* yang mengenkripsi atau mencuri data pada perangkat dan kemudian menuntut pembayaran uang tebusan kepada pemilik perangkat agar data tersebut dapat diakses kembali atau tidak dibocorkan (Rimbarawa et al., 2021). Sedangkan *malware* adalah perangkat lunak yang sengaja dirancang untuk melakukan tindakan berbahaya atau merusak terhadap perangkat lunak lainnya. Tujuannya dapat mencakup penyadapan, pencurian informasi pribadi, hingga perusakan sistem pada perangkat korban oleh pihak yang tidak sah (Kramer & Bradfield, 2010), (Cahyanto et al., 2017).

Serangan ini dimulai dari server basis data utama perusahaan dan menyebar ke komputer staf TI. Serangan ini menjadi titik balik penting yang mendorong perusahaan untuk meningkatkan kebijakan dan praktik keamanan informasi.

Untuk mengatasi tantangan ini, perusahaan telah mempertimbangkan menerapkan kerangka kerja CIS *Critical*

DOI: https://doi.org/10.33020/saintekom.v14i1.610
Lisensi: CC BY-SA 4.0 | Copyright © 2024, Penulis

Security Controls atau CIS *Controls* yang dikembangkan oleh Center for Internet Security (CIS) (Center for Internet Security, 2021), (Center for Internet Security, t.t.). Kerangka kerja ini dipilih karena lebih bersifat teknis dan menawarkan fleksibilitas implementasi yang dapat disesuaikan dengan kebutuhan perusahaan melalui Grup Implementasi (*Implementation Group*). CIS *Controls* juga menekankan diterapkannya *host-based firewall* dan sistem pencadangan yang dapat mengurangi risiko serangan *ransomware* dan memfasilitasi respons terhadap insiden keamanan(Shamma, 2018). Selain CIS *Controls*, ada juga opsi lain seperti NIST *Cybersecurity Framework* dan standar ISO/IEC 27001:2022 yang dapat meningkatkan keamanan siber di perusahaan.

NIST *Cybersecurity Framework*, yang dikeluarkan oleh *National Institute of Standards and Technology* (NIST), banyak digunakan di Amerika Serikat. Kerangka kerja ini memiliki struktur dan format yang mudah diimplementasikan di perusahaan. Namun, kerangka kerja ini terbilang usang, karena versi terakhir diperbarui pada tahun 2018 dan beberapa kontrolnya tidak lagi relevan di masa sekarang. Selain itu, NIST *Cybersecurity Framework* juga memiliki kekurangan, seperti penyimpanan log yang singkat sehingga dapat menyulitkan penyidik forensik untuk menemukan adanya pelanggaran keamanan yang umumnya baru ditemukan sekitar empat bulan setelah kejadian. Penggunaan SaaS (*Software as a Services*) atau PaaS (*Platform as a Services*) pada NIST *Cybersecurity Framework* juga dapat meningkatkan risiko keamanan karena tanggung jawab diserahkan kepada pihak ketiga yang keamanannya belum tentu terjamin (Sam Bocetta, 2021).

ISO/IEC 27001:2022 adalah standar keamanan informasi terbaru dari ISO dan digunakan secara global (Sama et al., 2021). Meskipun telah diperbarui untuk mengatasi tantangan keamanan siber saat ini, implementasinya membutuhkan pertimbangan matang, terutama untuk perusahaan kecil dengan 10-15 karyawan, karena standar ini mengharuskan penerapan seluruh klausulnya. Standar ini bertujuan meningkatkan kerahasiaan, integritas dan ketersediaan informasi dalam segala konteks (Februari & Fitria, 2019).

Dengan memahami permasalahan dan isu-isu ini, penelitian ini bertujuan untuk membantu perusahaan dalam menghadapi ancaman

DOI: https://doi.org/10.33020/saintekom.v14i1.610
Lisensi: CC BY-SA 4.0 | Copyright © 2024, Penulis

siber dengan lebih baik melalui pengukuran, analisis dan usulan rekomendasi dalam rangka meningkatkan keamanan siber di perusahaan. Hasil penelitian ini diharapkan dapat memberikan kontribusi positif dalam meningkatkan kesadaran dan praktik keamanan siber di perusahaan, serta membantu mencegah terjadinya serangan siber serupa di masa depan.

Beberapa penelitian terdahulu yang berkaitan dengan penggunaan CIS *Controls* dalam penerapan praktik keamanan siber pernah dilakukan oleh beberapa peneliti, antara lain penelitian yang menganalisis kerentanan pada *Vulnerable Docker* Menggunakan *Alienvault* dan *Docker Bench for Security* dengan mengacu pada *framework* CIS Control (Hanifah et al., 2021). Penelitian ini bertujuan untuk menguji secara empiris tentang analisis kerentanan pada Docker menggunakan pemindai kerentanan yang mengacu pada *framework* CIS *Control* yang didasarkan pada CIS *Docker Benchmark* v1.3.1. Pada penelitian ini, CIS Control tersebut digunakan dalam rangka mengurangi risiko keamanan yang mungkin muncul pada penelitian ini.

Kemudian yang berikutnya adalah perancangan dan implementasi sistem *Security Control Assessment* berbasis *web* (Prabaswara, 2020). Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem *Security Control Assessment* berbasis web yang dapat melakukan kontrol dan manajemen dari penerapan standar keamanan CIS *Controls* di perusahaan.

Penelitian lainnya yang berkaitan dengan CIS *Controls*, namun lebih spesifik pada penggunaan CIS *Benchmark*s, yaitu penelitian mengenai penggunaan CIS *Benchmark* sebagai *security auditor* untuk mengaudit layanan SaaS (Najib et al., 2022). Hasil dari penelitian ini menyatakan bahwa CIS *Benchmark* dapat mendukung system administrator dalam melaksanakan evaluasi dari layanan SaaS dengan menggunakan hasil audit berdasarkan CIS *Benchmark* sebagai dokumen pendukung dalam melakukan langkah evaluasi.

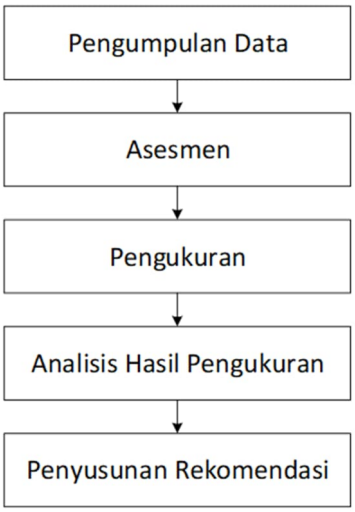
2. METODE

Penelitian ini fokus pada pengukuran tingkat keamanan siber di sebuah perusahaan TI di Jakarta dengan

DOI: https://doi.org/10.33020/saintekom.v14i1.610
Lisensi: CC BY-SA 4.0 | Copyright © 2024, Penulis

menggunakan kerangka kerja CIS *Controls*.

Gambar 1 menunjukkan tahapan penelitian yang berlangsung selama dua bulan. Tahapan tersebut mencakup pengumpulan data, asesmen, pengukuran, analisis, penyusunan rekomendasi, validasi, dan penyusunan laporan.



Gambar 1. Tahapan Penelitian

Data dikumpulkan melalui wawancara, observasi dan analisis dokumen terkait kebijakan dan prosedur keamanan yang sudah diterapkan di perusahaan. Asesmen dilakukan terhadap praktik keamanan siber perusahaan dengan menggunakan kerangka kerja CIS *Controls* versi 8 untuk seluruh kontrol dalam *Implementation Group 1 (IG1)*.

Grup implementasi ini perlu ditetapkan di awal untuk mengidentifikasi kontrol yang perlu diimplementasikan, dengan setiap IG sudah mencakup beberapa langkah pengamanan (*safeguards*) yang disesuaikan dengan profil risiko dan sumber daya perusahaan. Selain IG1, terdapat juga IG2 dan IG3 yang detailnya dapat dijelaskan sebagai berikut.

IG1 dalam CIS *Controls* mencakup organisasi skala kecil hingga menengah yang memiliki keterbatasan dalam sumber daya teknologi informasi dan keamanan siber. Fokus utamanya adalah memastikan kelangsungan operasional bisnis. Kelompok Implementasi ini terdiri dari kontrol-kontrol yang dianggap sebagai "*essential cyber hygiene*" di dalam organisasi, dengan total 56 langkah pengamanan (*safeguards*) dalam 15 kontrol keamanan. Langkah-langkah ini memungkinkan organisasi untuk mengenali, melindungi, mendeteksi, menanggapi dan pulih dari ancaman siber (*Center for Internet Security*, 2021), (*Center for Internet Security*, 2023).

Berbeda dengan IG1, *Implementation Group 2* (IG2) dalam CIS *Controls* mencakup organisasi yang telah mempekerjakan individu yang memiliki tanggung jawab untuk

DOI: https://doi.org/10.33020/saintekom.v14i1.610
Lisensi: CC BY-SA 4.0 | Copyright © 2024, Penulis

mengelola dan melindungi infrastruktur TI, serta menyimpan serta memproses informasi rahasia pelanggan atau organisasi. Grup Implementasi ini mencakup semua kontrol yang terdapat di IG1, ditambah dengan tiga kontrol dan 74 *safeguards* yang diperlukan untuk mengatasi kompleksitas operasional yang lebih tinggi (Center for Internet Security, 2021).

Sedangkan *Implementation Group 3* (IG3) dalam CIS *Controls* mencakup organisasi yang memiliki ahli keamanan yang mengkhususkan diri dalam berbagai aspek keamanan siber. Grup Implementasi ini mencakup semua kontrol yang terdapat di IG1 dan IG2, serta 23 *safeguards* tambahan dalam 18 kontrol keamanan untuk mengatasi risiko yang lebih tinggi (Center for Internet Security, 2021).

Seperti yang sudah dijelaskan sebelumnya, dari total 18 kontrol keamanan dalam CIS *Controls*, asesmen hanya mengacu pada 15 kontrol keamanan yang akan dievaluasi sesuai dengan kontrol yang direkomendasikan untuk *Implementation Group 1*, di mana kontrol 13, 16 dan 18 tidak termasuk di dalamnya. Detail seluruh kontrol dalam CIS *Controls* versi 8 dapat dilihat pada Tabel 1.

Tabel 1. Daftar Kontrol dalam CIS *Controls*

CIS *Control*	Deskripsi
1	Inventory and Control of Enterprise Assets
2	Inventory and Control of Software Assets
3	Data Protection
4	Secure Configuration of Enterprise Assets and Software
5	Account Management
6	Access Control Management
7	Continuous Vulnerability Management
8	Audit Log Management
9	*Email* and *Web Browser* Protections
10	Malware Defenses
11	Data Recovery
12	Network Infrastructure Management
13	Network Monitoring and Defense
14	Security Awareness and Skills Training
15	Service Provider Management
16	Application Software Security
17	Incident Response Management
18	Penetration Testing

(Sumber: Center for Internet Security, 2021)

Hasil asesmen diukur dan dianalisis untuk mengidentifikasi kelemahan dan risiko keamanan siber. Rekomendasi strategis disusun untuk meningkatkan praktik keamanan siber dan kemudian divalidasi dan diverifikasi untuk keakuratannya. Terakhir, hasil penelitian disajikan dalam bentuk laporan kepada pihak terkait di perusahaan untuk membantu memperkuat sistem keamanan siber mereka.

Dalam proses asesmen, ada empat pertanyaan utama yang digunakan

DOI: https://doi.org/10.33020/saintekom.v14i1.610
Lisensi: CC BY-SA 4.0 | Copyright © 2024, Penulis

untuk menilai sejauh mana perusahaan telah menerapkan kontrol keamanan CIS. Pertanyaan-pertanyaan tersebut terkait apakah perusahaan memiliki kebijakan tertulis untuk kontrol tersebut, apakah kontrol tersebut sudah diimplementasikan di perusahaan, apakah kontrol tersebut sudah diotomatisasi untuk pelaksanaannya dan apakah hasil dari pelaksanaan kontrol tersebut dilaporkan kepada pihak manajemen.

Pertanyaan ini membantu dalam menilai praktik keamanan siber di perusahaan dan menentukan apakah perlu perbaikan atau tindakan tambahan. Responden menjawab dengan pilihan jawaban yang telah disediakan.

Ada dua pengukuran penting yang dilakukan dalam penelitian ini, yakni pengukuran Skor Grup Implementasi dan tingkat kematangan. Skor Grup Implementasi adalah nilai rata-rata dari seluruh skor Grup Implementasi per kontrol keamanan yang terpilih di suatu Grup Implementasi. Skor ini mencerminkan sejauh mana implementasi kontrol keamanan telah diterapkan di suatu Grup Implementasi dan memberikan gambaran keseluruhan tentang kesiapan organisasi dalam menghadapi ancaman siber. Skor Grup Implementasi ini memiliki rentang nilai 0-100%.

Model pengukuran tingkat kematangan yang digunakan dalam kerangka kerja CIS *Controls* memiliki perbedaan dengan sebagian besar model kematangan yang umumnya mengacu pada model CMMI (*Capability Maturity Model Integration*). Dalam CIS *Controls*, tingkat kematangan mencerminkan sejauh mana organisasi telah menerapkan praktik kontrol keamanan tertentu. Perbedaan ini menghasilkan deskripsi yang unik untuk tingkat kematangan dalam CIS *Controls*. Detailnya dapat dilihat pada Tabel 2.

Tabel 2. Deskripsi Tingkat Kematangan CIS *Controls*

Tingkat Kematangan	Deskripsi	Keterangan
Level 1	Kebijakan Lengkap	Level ini menunjukkan seberapa lengkap kebijakan keamanan yang telah disusun oleh organisasi.
Level 2	Kontrol 1–5 Diterapkan	Level ini menunjukkan sejauh mana organisasi telah mengimplementasikan kontrol 1–5.
Level 3	Semua Kontrol Diterapkan	Level ini menunjukkan sejauh mana organisasi telah mengimplementasikan seluruh kontrol yang diperlukan.

DOI: https://doi.org/10.33020/saintekom.v14i1.610
Lisensi: CC BY-SA 4.0 | Copyright © 2024, Penulis

Tingkat Kematangan	Deskripsi	Keterangan
Level 4	Semua Kontrol Terotomatisasi	Level ini menunjukkan sejauh mana organisasi telah mengotomatisasikan seluruh kontrol yang diimplementasikan.
Level 5	Semua Kontrol Dilaporkan	Level ini menunjukkan sejauh mana organisasi telah melaporkan seluruh kontrol yang diimplementasikan.

(Sumber: Center for Internet Security, 2021)

Nilai maksimum tingkat kematangan yang bisa dicapai oleh masing-masing Grup Implementasi, yaitu IG1, IG2 dan IG3 dapat dilihat dalam Tabel 3.

Penentuan nilai dalam rentang 0-1 pada tiap level dapat dijelaskan sebagai berikut. Skor pada Level 1 dihitung berdasarkan rata-rata status kebijakan di seluruh Grup Implementasi. Skor pada Level 2 dihitung berdasarkan rata-rata status pelaksanaan kontrol 1-5 dalam masing-masing Grup Implementasi. Skor pada Level 3 dihitung berdasarkan rata-rata status pelaksanaan kontrol 6-18 dalam setiap Grup Implementasi. Skor pada Level 4 dihitung berdasarkan rata-rata status kontrol yang telah diotomatisasi di masing-masing Grup Implementasi. Sedangkan skor pada Level 5 dihitung berdasarkan rata-rata status pelaporan kontrol dalam setiap Grup Implementasi.

Tabel 3. Nilai Maksimum Tingkat Kematangan Setiap Grup Implementasi

Tingkat Kematangan	Deskripsi	Skor (Skala 0 – 1)		
		IG1	IG2	IG3
Level 1	Kebijakan Lengkap	0,37	0,85	1,00
Level 2	Kontrol 1-5 Diterapkan	0,50	0,89	1,00
Level 3	Semua Kontrol Diterapkan	0,31	0,83	1,00
Level 4	Semua Kontrol Terotomatisasi	0,34	0,85	1,00
Level 5	Semua Kontrol Dilaporkan	0,34	0,85	1,00
Peringkat Kematangan (Skala 0 – 5)		1,86	4,27	5,00

(Sumber: Center for Internet Security, 2021)

Peringkat tingkat kematangan keseluruhan diperoleh dengan menggabungkan skor tingkat kematangan dari setiap Grup Implementasi, menggunakan skala 0 hingga 5 sebagai referensi. Hasil peringkat ini akan menjadi panduan bagi perusahaan dalam meningkatkan kemampuan pencegahan dan pendeteksian terhadap ancaman keamanan siber, serta mengevaluasi kemajuan implementasi kerangka kerja CIS *Controls* secara keseluruhan. Setiap Grup Implementasi memiliki nilai maksimum yang berbeda, sesuai dengan jumlah *safeguard* yang

DOI: https://doi.org/10.33020/saintekom.v14i1.610
Lisensi: CC BY-SA 4.0 | Copyright © 2024, Penulis

diimplementasikan. Sebagai contoh, IG1 hanya mengimplementasikan 56 *safeguard*, dengan nilai maksimum yang lebih rendah dari pada IG2 yang mengimplementasikan 130 *safeguard*, atau IG3 yang menerapkan 153 *safeguard*. IG3 merupakan Grup Implementasi yang menerapkan semua *safeguard*, sehingga mencapai nilai maksimum tertinggi, yaitu 1, karena tingkat penerapan kontrol keamanan yang lebih komprehensif. Semakin banyak *safeguard* yang diimplementasikan, semakin tinggi potensi nilai kematangan yang dapat dicapai oleh Grup Implementasi tersebut.

3. HASIL DAN PEMBAHASAN

Tingkat kematangan praktik keamanan siber di perusahaan, sebagaimana diperlihatkan dalam Tabel 4, menunjukkan bahwa masih ada banyak ruang untuk peningkatan.

Pada Level 1, implementasi kebijakan keamanan perlu ditingkatkan karena belum semua aspek kebijakan diterapkan secara konsisten. Level 2 menunjukkan langkah awal yang positif dengan kontrol-kontrol dasar yang telah diterapkan, tetapi masih ada ruang untuk peningkatan. Di Level 3, hampir semua kontrol telah diterapkan, kecuali manajemen log audit. Level 4 menunjukkan sebagian kontrol telah terotomatisasi, tetapi masih ada ruang untuk peningkatan.

Tabel 4. Hasil Pengukuran Tingkat Kematangan

Tingkat Kematangan	Deskripsi	Skor (0–1)	
		Kematangan	Maksimum
Level 1	Kebijakan Lengkap	0,04	0,37
Level 2	Kontrol 1–5 Diterapkan	0,20	0,50
Level 3	Semua Kontrol Diterapkan	0,10	0,31
Level 4	Semua Kontrol Terotomatisasi	0,07	0,34
Level 5	Semua Kontrol Dilaporkan	0,01	0,34
Peringkat Kematangan (Skala 0–5)		0,41	1,86

Pada Level 5, hanya sebagian kecil praktik keamanan yang dilaporkan ke manajemen. Dalam analisis keseluruhan, nilai peringkat kematangan keamanan siber 0,41 yang diperoleh masih sangat rendah, sehingga perusahaan perlu berfokus pada perbaikan implementasi kebijakan dan kontrol serta meningkatkan kematangan keamanan siber secara keseluruhan.

Hasil pengukuran Skor Grup Implementasi untuk IG1 adalah 36%,

DOI: https://doi.org/10.33020/saintekom.v14i1.610
Lisensi: CC BY-SA 4.0 | Copyright © 2024, Penulis

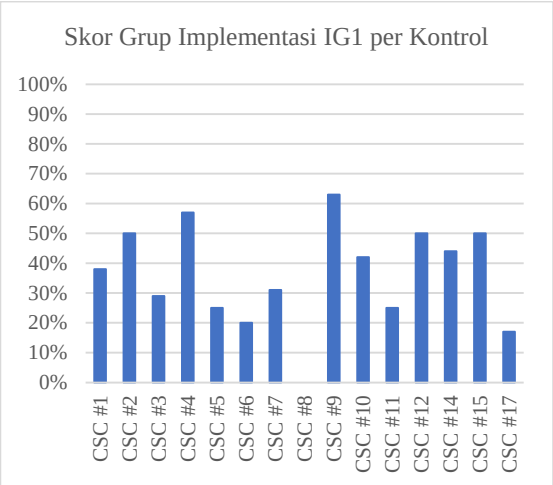
menunjukkan bahwa masih banyak *safeguards* yang belum sepenuhnya diterapkan. Detailnya dapat dilihat pada Tabel 5.

Tabel 5. Skor IG1 Per Kontrol

CIS Control	Skor (%)
CSC #01 - Inventory and Control of Enterprise Assets	38
CSC #02 - Inventory and Control of Software Assets	50
CSC #03 - Data Protection	29
CSC #04 - Secure Configuration of Enterprise Assets and Software	57
CSC #05 - Account Management	25
CSC #06 - Access Control Management	20
CSC #07 - Continuous Vulnerability Management	31
CSC #08 - Audit Log Management	0
CSC #09 - *Email* and *Web Browser* Protections	63
CSC #10 - Malware Defenses	42
CSC #11 - Data Recovery	25
CSC #12 - Network Infrastructure Management	50
CSC #14 - Security Awareness and Skills Training	44
CSC #15 - Service Provider Management	50
CSC #17 - Incident Response Management	17
Skor Grup Implementasi	36

Beberapa kontrol, seperti Proteksi *Email* dan *Web Browser* (CSC #09), Konfigurasi Aman pada Aset dan Perangkat Lunak Perusahaan (CSC #04) dan Manajemen Infrastruktur Jaringan (CSC #12), telah diterapkan dengan baik, mencapai skor implementasi tertinggi. Namun, ada tiga kontrol dengan skor terendah, yaitu Manajemen Log Audit (CSC #08) dengan nilai 0%, kemudian diikuti oleh Manajemen Respons Insiden (CSC #17) dan Manajemen Kontrol Akses (CSC #06) yang hanya mencapai skor masing-masing 17% dan 20%. Perusahaan perlu memprioritaskan perbaikan pada ketiga kontrol ini untuk mengurangi potensi risiko keamanan siber dan meningkatkan perlindungan data dan sistem. Skor Grup Implementasi akan menjadi acuan untuk perbaikan keamanan siber di masa mendatang.

Gambar 2 menunjukkan Skor Grup Implementasi IG1 per Kontrol jika divisualisasikan dalam bentuk grafik batang.



Gambar 2. Grafik Batang Skor Grup Implementasi IG1 per Kontrol.

DOI: https://doi.org/10.33020/saintekom.v14i1.610
Lisensi: CC BY-SA 4.0 | Copyright © 2024, Penulis

Hasil ini dapat mengidentifikasi area yang perlu perbaikan dan peningkatan dalam upaya meningkatkan keamanan siber organisasi. Oleh karena itu, tindakan korektif dan peningkatan harus dilakukan secara selektif pada kontrol-kontrol tertentu guna meningkatkan kematangan keamanan siber secara keseluruhan di masa mendatang.

4. KESIMPULAN

Hasil evaluasi terhadap tingkat kematangan praktik keamanan siber pada perusahaan TI di Jakarta dengan menggunakan kerangka kerja CIS *Controls* versi 8 menunjukkan tingkat kematangan yang sangat rendah. Risiko ancaman siber sebagian besar diterima tanpa penanganan signifikan, sementara sebagian besar kontrol dalam IG1 telah diterapkan secara informal tanpa kebijakan tertulis. Beberapa kontrol, seperti Proteksi *Email* dan *Web Browser* (CSC #09), Konfigurasi Aman pada Aset dan Perangkat Lunak Perusahaan (CSC #04) dan Manajemen Infrastruktur Jaringan (CSC #12), memiliki implementasi yang lebih baik, tetapi ada juga kontrol dengan implementasi rendah, seperti Manajemen Log Audit (CSC #08), Manajemen Respons Insiden (CSC #17) dan Manajemen Kontrol Akses (CSC #06).

Untuk meningkatkan praktik keamanan siber, perusahaan harus memperbaiki kontrol yang memiliki skor implementasi rendah, mengalokasikan sumber daya tambahan dan memberikan pelatihan yang intensif kepada karyawan. Pendekatan berkelanjutan dalam pemantauan dan evaluasi diperlukan dengan pembuatan kebijakan resmi yang disahkan oleh manajemen. Melibatkan semua pihak terkait dalam langkah-langkah perbaikan akan memungkinkan perusahaan untuk membangun fondasi yang lebih kuat dalam menghadapi tantangan keamanan siber di masa depan.

DAFTAR PUSTAKA

Amazon Web Service. (2023). *What Is Cybersecurity?* Amazon Web Services. https://aws.amazon.com/what-is/cybersecurity/

Cahyanto, T. A., Wahanggara, V., & Ramadana, D. (2017). Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis. *Jurnal Sistem & Teknologi Informasi Indonesia*, *2*(1). https://doi.org/10.32528/justindo.v2i1.1037

Center for Internet Security. (t.t.). *About us*. Center for Internet Security.

DOI: https://doi.org/10.33020/saintekom.v14i1.610
Lisensi: CC BY-SA 4.0 | Copyright © 2024, Penulis

Diambil 27 Desember 2022, dari https://www.cisecurity.org/about-us/

Center for Internet Security. (2021). *CIS Critical Security Controls Version 8*. Center for Internet Security.

Center for Internet Security. (2023). *The Cost of Cyber Defense CIS Controls Implementation Group 1* (V. Stocchetti & T. Sager, Ed.). Center for Internet Security. https://www.cisecurity.org/controls/

Februari, P., & Fitria. (2019). Audit Sistem Keamanan Informasi Menggunakan ISO 27001 pada SMKN 1 Pugung, Lampung. *Jurnal CoreIT*, *5*(2), 44–48. https://doi.org/10.24014/coreit.v5i2.8276

Hanifah, F., Budiyono, A., & Widjajarto, A. (2021). Analisa Kerentanan pada Vulnerable Docker Menggunakan Alienvault dan Docker Bench for Security dengan Acuan Framework CIS Control. *e-Proceeding of Engineering*, *8*(5), 8879–8885. https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/15914

Kramer, S., & Bradfield, J. C. (2010). A General Definition of Malware. *Journal in Computer Virology*, *6*(2), 105–114. https://doi.org/10.1007/s11416-009-0137-1

Najib, M., Purnomosidi D.P, B., & Nugroho, M. A. (2022). Implementasi Security Auditor untuk Standardisasi Instalasi Server pada Layanan SaaS Menggunakan CIS *Benchmark*. *Cyber Security dan Forensik Digital*, *5*(2), 83–88. https://doi.org/10.14421/csecurity.2022.5.2.3929

Prabaswara, J. (2020). *Perancangan dan Implementasi Sistem Security Control Assessment Berbasis Web* [Universitas Esa Unggul]. https://digilib.esaunggul.ac.id/perancangan-dan-implementasi-sistem-security-control-assessment-berbasis-web-19673.html

Rimbarawa, Z. I., Kholisoh, E., Rahmayani, Z. P., & Redaksi, D. (2021). Systematic Literature Review: Permasalahan Ransomware pada Aplikasi Berbasis Cloud. *JURNAL INTECH*, *2*(2), 19–22. https://doi.org/10.54895/intech.v2i2.877

Sam Bocetta. (2021, Maret 3). *3 Security Issues Overlooked by the NIST Framework*. Network Computing. https://www.networkcomputing.com/network-security/3-security-issues-overlooked-nist-framework

Sama, H., Licen, L., Saragi, J. S. D., Erline, M., Kelvin, K., Hartanto, Y., Winata, J., & Devalia, M. (2021). Studi Komparasi Framework NIST dan ISO 27001 Sebagai Standar Audit Dengan Metode Deskriptif Studi Pustaka. *Rabit: Jurnal Teknologi dan Sistem Informasi Univrab*, *6*(2), 116–121. https://doi.org/10.36341/rabit.v6i2.1752

Shamma, B. (2018). *Implementing CIS Critical Security Controls for Organizations on a Low-Budget* (Nomor December) [University of Houston]. https://hdl.handle.net/10657/4048

DOI: https://doi.org/10.33020/saintekom.v14i1.610
Lisensi: CC BY-SA 4.0 | Copyright © 2024, Penulis