Smart Comp: Jurnalnya Orang Pintar Komputer
Volume 13, Nomor 4, Oktober 2024, hlm. 809-814
Terakreditasi Sinta, Peringkat 4, SK No. 105/E/KPT/2022
DOI : 10.30591/smartcomp.v13i4.6865

P-ISSN : 2089-676X
E-ISSN : 2549-0796

Evaluasi Manajemen Insiden Keamanan Informasi Menggunakan Framework ISO/IEC 27035 dan Crest pada Instansi XYZ

Ismail Yusry*1, Kalamullah Ramli2
Universitas Indonesia
Email: *1ismail.yusry@ui.ac.id, 2kalamullah.ramli@ui.ac.id

(Naskah masuk: *7 Juni 2024*, diterima untuk diterbitkan: *24 September 2024*)

Abstrak: *Saat ini insiden terhadap keamanan informasi sangat sering terjadi pada instansi pemerintah. Insiden tersebut dapat berupa serangan denial of service (dos), malware, kebocoran data dan web defacement. Jika tidak ditangani secara benar maka serangan tersebut tentu dapat mempengaruhi layanan informasi, sehingga diperlukan kesiapan dari instasi pemerintah untuk dapat mengantisipasinya. Untuk menjaga kepercayaan masyarakat terhadap pemerintah tetap tinggi, pemerintah wajib untuk dapat memberikan layanan publik berupa sistem informasi yang mudah dan cepat untuk diakses. Salah satu langkah yang dilakukan oleh instansi XYZ untuk mengantispasi adanya insiden keamanan informasi yaitu dengan membentuk CSIRT (Computer Security Incident Response Team). Tim tersebut diharapkan untuk dapat melakukan manajemen insiden keamanan informasi. Agar dapat bekerja secara optimal perlu dilakukan evaluasi terhadap tim. Penelitian ini akan melakukan evaluasi terhadap organisasi ditinjau dari aspek organisasi, teknologi, orang dan proses dengan berdasarkan ISO / IEC 27035 selain itu dilakukan pengukuran tingkat kematangan menggunakan dengan model CREST. Hasil asesmen menggunakan ISO/IEC 27035 menunjukkan bahwa instansi XYZ telah menerapkan klausul sebesar 54% sedangkan pengukuran tingkat kematangan penanganan insiden dengan menggunakan model CREST instansi adalah 3,1 dari skala 5.*

Kata Kunci – *Insiden Keamanan Informas; Manajemen Insiden; CSIRT; ISO 2703; CREST*

Evaluation of Information Security Incident Management Using ISO/IEC 27035 and CREST Frameworks at XYZ Institution

Abstract: *Currently, information security incidents occur very often in government agencies. These incidents can take the form of denial of service (DOS) attacks, malware, data leaks and web defacement. If not handled properly, these attacks can certainly affect information services, so government agencies need to be prepared to be able to anticipate them. To maintain public trust in the government remains high, the government is obliged to be able to provide public services in the form of information systems that are easy and fast to access. One of the steps taken by the XYZ agency to anticipate information security incidents is by forming a CSIRT (Computer Security Incident Response Team). The team is expected to be able to carry out information security incident management. In order to work optimally, it is necessary to evaluate the team. This research will evaluate the organization in terms of organizational, technological, people and process aspects based on ISO / IEC 27035, in addition to measuring the level of maturity using the CREST model. The results of the assessment using ISO/IEC 27035 are that the XYZ agency has implemented the clause by 54% while the measurement of the maturity level of incident handling using the using CREST model is 3.1 on a scale of 5.*

Keywords – *Security Incident; Incident Management; CSIRT; ISO 27035; CREST*

1. PENDAHULUAN

Dalam era teknologi yang semakin maju, ancaman terhadap keamanan informasi menjadi semakin kompleks dan meluas [7]. Insiden seperti peretasan, pencurian data, dan serangan malware telah menjadi ancaman serius bagi organisasi di seluruh dunia, termasuk di Indonesia. Insiden keamanan terhadap informasi dapat terjadi termasuk pada lembaga pemerintahan, insiden tersebut dapat terjadi kapan saja, oleh karena itu setiap organisasi baik itu kecil, menengah dan besar perlu mempunyai deteksi dan respon terhadap insiden dengan baik [10]. Kejadian insiden keamanan informasi bisa terjadi dan menimbulkan dampak negatif, seperti kerugian, masalah hukum dan

kepercayaan terhadap organisasi. Organisasi perlu memiliki mekanisme yang efektif dalam mendeteksi, menanggapi, dan mengelola insiden keamanan guna melindungi aset informasinya [14]. Berdasarkan laporan dari BSSN selama tahun 2023 tercatat 4 juta APT (Advanced Persistent Threat) dan 1 juta aktivitas ransowmare. Angka tersebut bisa dikatakan sangat tinggi mengingat dampak yang ditimbulkannya. Saat ini APT merupakan tantangan keamanan untuk organisasi karena sifatnya yang canggih dan sophisticated.

Sesuai dengan Peraturan Presiden nomor 95 tahun 2018, Sistem Pemerintahan Berbasis Elektronik merupakan pemerintah yang menggunakan teknologi informasi dan komunikasi pada layanannnya. SPBE mengamanatkan bahwa layanan sistem elektronik harus menggunakan prinsip mengenai keamanan. Instansi XYZ, sebagai salah satu lembaga pemerintah yang membidangi urusan luar negeri merupakan instansi yang mengelola informasi sensitif dan beberapakali menemui permasalahan terkait insiden keamanan informasi [6]. Sebagai salah satu organisasi yang sudah menerapkan layanan publik berupa sistem elektronik, instansi XZY memerlukan mekanisme agar tingkat ketersediaan terhadap sistem informasi tersebut dapat terjaga dengan baik. Dalam mengelola permasalahan keamanan instansi XYZ telah memiliki tim CSIRT yang membantu menangani insiden keamanan informasi. Menurut buku Corporate Computer Security insiden respon merupakan reaksi terhadap insiden sesuai dengan rencana yang sudah dibuat, sehingga diperlukan evaluasi terutama melihat kesiapan dari organisasi dalam menghadapi ada insiden keamanan [2].

Pengelolaan insiden keamanan informasi memerlukan pendekatan dalam penerapanannya. Salah satu pendekatannya adalah dengan menggunakan standar yang sudah diakui secara internasional. Beberapa standar yang digunakan untuk menjadi panduan dalam manajemen insiden keamanan informasi yaitu ITIL, ISO/IEC 27035, NIST SP 800-61, ENISA, dan SANS. Secara umum standar tersebut memiliki pedoman yang hampir sama. ISO 27035 merupakan standar yang dapat digunakan sebagai pijakan awal yang baik dalam hal penanganan insiden keamanan informasi.

Penelitian sebelumnya [8] melakukan penelitian kualitatif dengan membandingkan standar yang digunakan untuk mengukur tingkat kematangan penanganan insiden siber yaitu CREST dan SIM3 [3]. Sedangkan pada penelitian lainnya [13] melakukan penelitian perancangan manajemen insiden dengan menggunakan standar ISO / IEC 27035. Penelitian tersebut dilakukan dengan menggunakan metode kualitatif berupa studi kasus [13].

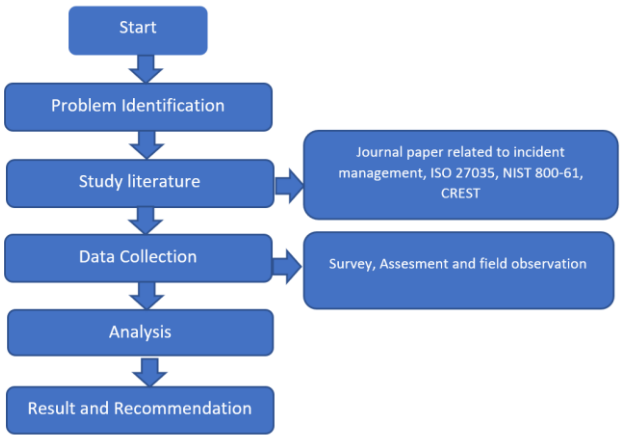
Dari penelitian-penelitian tersebut belum terdapat penelitian yang menggunakan framework CREST sebagai studi kasus dan kemudian menggabungkannya dengan ISO / IEC 27035 untuk dapat digunakan sebagai evaluasi penanganan insiden keamanan informasi pada organisasi seperti di pemerintahan [12].

2. METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif berupa studi kasus di lingkungan instansi XYZ. Penelitin ini diawali dengan identifikasi permasalahan terkait pengelolaan insiden keamanan. Penelitian ini dilakukan mengikuti tahapan penelitian yang ditunjukkan pada Gambar 1.

Step 1: Penelitian dimulai dengan identifikasi masalah. Prosesnya dilakukan dengan melihat permasalahan yang terjadi dilingkungan instansi XYZ dimana dijumpai bahwa masih banyaknya permasalahan terkait adanya serangan berupa malware dan phising pada infrastruktur jaringan instansi XYZ. Step 2: Setelah masalah teridentifikasi, dilakukan studi literatur untuk menemukan teori yang berkaitan dengan pengelolaan insiden keamanan informasi. Selama proses ini, peneliti melakukan studi untuk menemukan pendekatan terbaik dalam mengolah informasi dalam menjawab pertanyaan penelitian penelitian ini. Berdasarkan studi tersebut, dipilih pendekatan menggunakan ISO /IEC 27035 karena merupakan standar telah banyak digunakan dalam penanganan insiden keamanan informasi. Seperti dijelaskan diatas bahwa ISO / IEC 27035 terbagi menjadi 2 (dua) bagian di penelitian ini di bagian ISO 27035 bagian 1 dipilih klausul dari plan and prepare, detection and reporting, asesment and decision, response dan lesson learnt. Pemilihan klausul tersebut dikarenakan hal tersebut merupakan siklus dari penanganan

insiden. Step 3: Melakukan pengumpulan data yaitu dengan menggunakan metode survei dan wawancara. Step 4 : melakukan analisis data dari pengumpulan data tersebut. Tahap terakhir adalah berupa kesimpulan dari penelitian yang dapat dimanfaatkan oleh organisasi.



Gambar 1. Alur Penelitian

3. HASIL DAN PEMBAHASAN

3.1. Pembahasan

Dalam melakukan asesmen menggunakan ISO 27035 pada instansi XYZ, peneliti menggunakan penilaian skala seperti tabel berikut ini:

Table 1. Skala Penilaian

Skala	Implementasi penerapannya pada organisasi
1	penuh
0.5	parsial
0	tidak ada

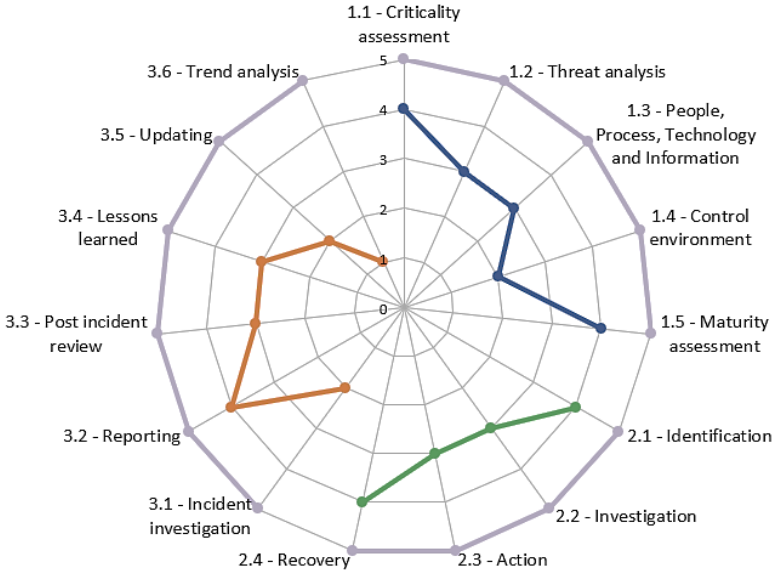
Dimana angka 0 menunjukan bahwa organisasi belum menerapkannya sama sekali, sedangkan nilai 0,5 menunjukkan bahwa organisasi menerapkan sebagian dan nilai 1 yaitu organisasi telah menerapkan secara menyeluruh klausul pada ISO 27035.

Klausul	Implementasi			Jumlah klausul
	penuh	parsial	tidak dilakukan	
ISO 27035:2016 Bagian 1				
5.2 Plan and Prepare	2	4	2	8
5.3 Detection and Reporting	5	1	2	8
5.4 Assesment and Decision	3	2	2	7
5.5 Response	4	10	2	16
5.6 Lesson Learnt	1	3	3	7
ISO 27035:2016 Bagian 2				
6.5 Incident classification scale		1		1
6.6 Incident forms			1	1
6.7 Processes and procedures	4	5	1	10
7.3 IRT Staff		4		4
12.2 Identifying Lessson Learned		2	1	3
12.5 IRT Evaluation	1	2	1	4
	20	34	15	69
Skala (0 -1)	20	17		37
Persentase penilaian				53 %

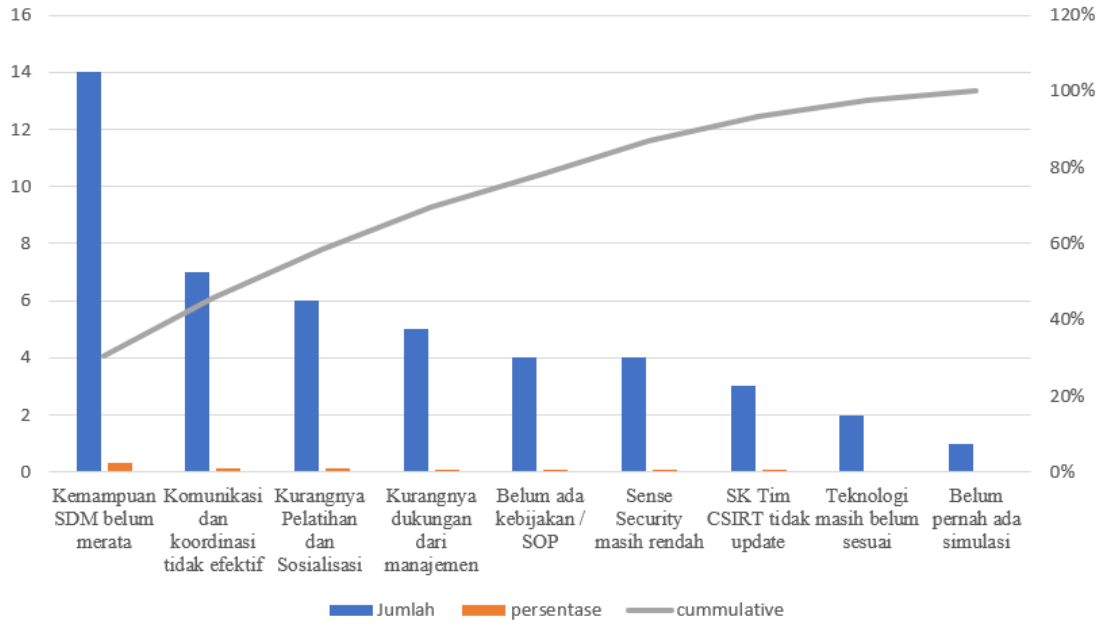
Gambar 2. Hasil Asesmen ISO/IEC 27035

Hasil asesmen dengan ISO 27035 menunjukkan bahwa dari 69 klausul , instansi XYZ telah melakukan implementasi sebesar 53%. Jika dilihat dari gambar, instansi XYZ cukup baik dalam melakukan detection dan reporting, hal tersebut karena organisasi sudah menerapkan berbagai perangkat pengamanan jaringan [1]. Disisi lain organisasi masih kurang dalam melakukan response hal ini terjadi karena sumber daya manusia baik dari sisi jumlah maupun keahlian dalam melakukan digital forensik masih terbatas [9]. Kemudian di bagian lesson learnt , organisasi masih kurang dalam menerapkan perbaikan pasca terjadinya insiden, sesuai panduan perlu dilakukan continues improvement terhadap tim CSIRT, proses, orang dan teknologi [11].

Hasil asesmen menggunakan CREST, instansi XYZ secara rata-rata mendapatkan nilai 3,1 dari skala 5 seperti dapat dilihat pada gambar dibawah ini. Beberapa hal yang sangat baik adalah organisasi selalu menerapkan critical assessment, maturity assessment, identification, recovery dan reporting namun masih kurang dalam hal control environtment, investigation, updating dan trend analysis [8].



Gambar 3. Hasil Pengukuran Tingkat Kematangan



Gambar 4. Hasil Survey Permasalahan

Penelitian ini juga melakukan survey terhadap beberapa pegawai yang memiliki pengetahuan di bidang TIK. Pertanyaan yang diajukan adalah hambatan apa yang dapat mempengaruhi penanganan insiden keamanan informasi instansi XYZ [4]. Dari grafik pareto chart dapat dilihat bahwa terdapat 3(tiga) permsalahan yang tinggi yaitu adalah kemampuan SDM (Sumber Daya Manusia) yang belum merata , komunikasi dan koordinasi yang belum efektif dan kurangnya pelatihan dan sosialisasi. Terkait dengan komunikasi dan koordinasi, dalam hal melakukan penanganan insiden seringkali tim harus melakukan koordinasi baik itu dengan internal organisasi seperti administrator aplikasi dan jaringan, pengguna layanan aplikasi dan juga faktor eksternal seperti dengan pihak satuan kerja yang memiliki tugas selain TIK [5].

4. KESIMPULAN

Berdasarkan hasil penelitian, penggunaan standar diperlukan untuk melakukan pendekatan penanganan insiden keamanan informasi. ISO/IEC 27035 merupakan standar yang sangat baik untuk menjadi panduan pada organisasi pemerintahan, sedangkan CREST dapat digunakan untuk mengukur tingkat kematangan insiden keamanan.

Hasil asesmen dengan ISO / IEC 27035 dan CREST menunjukkan bahwa instansi XYZ masih memerlukan perbaikan terutama disisi peningkatan kapasitas SDM dalam penanganan insiden keamanan, peningkatan security awarness seluruh pegawai dan pembuatan kebijakan atau SOP terkait penanganan insiden keamanan informasi.

DAFTAR PUSTAKA

[1] Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams - Challenges in supporting the organisational security function. Computers and Security, 31(5). https://doi.org/10.1016/j.cose.2012.04.001

[2] BSI. (2016). BS ISO/IEC 270135-1: Information technology - security techniques - information security incident management. Part 1 - principles of incident management. Bs Iso/Iec 27035-1:2016.

[3] Hendra, R., & Hanita, M. (2020). THE IMPLEMENTATION OF CYBER INCIDENT MANAGEMENT FRAMEWORKS IN INDONESIA. Jurnal Teknologi Informasi Dan Pendidikan, 13(2). https://doi.org/10.24036/tip.v13i2.326

[4] Jibril, M. (2021). IMPLEMENTASI E-GOVERNMENT KOTA PROBOLINGGO (STUDI PERATURAN PRESIDEN NOMOR 95 TAHUN 2018 TENTANG SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK). JIANA (Jurnal Ilmu Administrasi Negara), 19(3). https://doi.org/10.46730/jiana.v19i3.8002

[5] Johnston, D. D., Vanderstoep, S. W., Creswell, J. W., Källander, K., Tibenderana, J. K., Akpogheneta, O. J., Strachan, D. L., Hill, Z., Asbroek, A. H. A. T., Conteh, L., Kirkwood, B. R., Meek, S. R., Miyazaki, K., Nozaki, I., Seitio-Kgokgwe, O., Mashalla, Y., Seloilwe, E., Chida, N., Odiwuor, C. W., … Sommerville, I. (2018). Cloud-Based Software Engineering. Computers and Education, 2(1).

[6] Kusuma, A. J., Ilmar, A., Rahmawati, R., Setiawan, M. C. A., & Murtasidin, B. (2024). MEMBANGUN DESA CERDAS PEMILU UNTUK MEWUJUDKAN PEMILU TAHUN 2024 YANG IDEAL DI DESA TEBING, KECAMATAN KELAPA, KABUPATEN BANGKA BARAT. Jurnal Pengabdian Masyarakat Multidisiplin, 7(2). https://doi.org/10.36341/jpm.v7i2.4097

[7] Lavrov, E. A., Zolkin, A. L., Aygumov, T. G., Chistyakov, M. S., & Akhmetov, I. V. (2021). Analysis of information security issues in corporate computer networks. IOP Conference Series: Materials Science and Engineering, 1047(1). https://doi.org/10.1088/1757-899X/1047/1/012117

[8] Lekota, F., & Coetzee, M. (2019). Cybersecurity incident response for the sub-Saharan African aviation industry. 14th International Conference on Cyber Warfare and Security, ICCWS 2019.

[9] Mat, N. I. C., Jamil, N., Yusoff, Y., & Kiah, M. L. M. (2024). A systematic literature review on advanced persistent threat behaviors and its detection strategy. In Journal of Cybersecurity (Vol. 10, Issue 1). https://doi.org/10.1093/cybsec/tyad023
[10] Pemerintah Pusat. (2018). Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. Menteri Hukum Dan Hak Asasi Manusia Republik Indonesia.
[11] Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. Computers and Security, 45. https://doi.org/10.1016/j.cose.2014.05.003
[12] UU Republik Indonesia, Munawir, M., Nasional, B. S., Susanta, G., Jatimnet.com, MajaMojokerto.net, Radarmojokerto.jawapos.com, Wijayakusuma, D. M. S., Nahman, A., Godfrey, L., Jacobsen, R., Buysse, J., Gellynck, X., Bayu, D., Depkes, R., Soekidjo Notoatmodjo, Boulanger, L., Ismoyo, I. H., Tarigan, R., … Sanyal, S. (2022). PENENTUAN ALTERNATIF LOKASI TEMPAT PEMBUANGAN AKHIR (TPA) SAMPAH DI KABUPATEN SIDOARJO. Energies, 15(1).
[13] Wikankara, Hartanto, R., & Nugroho, L. E. (2020). Perancangan Sistem Manajamen Insiden Keamanan Informasi Berdasarkan SNI ISO/IEC 27035 Di Instansi Pemerintah. Jurnal Teknologi Technoscientia, 13(1).
[14] Young, C. (2020). Incident Response Models. ISACA JOURNAL, 4.