Evaluasi Tata Kelola Keamanan Informasi Berdasarkan Standar ISO/IEC 27001:2013 dengan Menggunakan Model SSE-CMM (*System Security Engineering Capability Maturity Model*) pada Perusahaan Daerah Air Minum Surya Sembada Kota Surabaya

Dimas Pramudya Haqqi, Khakim Ghozali, dan Raden Venantius Hari Ginardi
Departemen Teknologi Informasi, Institut Teknologi Sepuluh Nopember (ITS)
e-mail: khakim@is.its.ac.id

***Abstrak*—PDAM Surya Sembada Kota Surabaya salah satu BUMD (Badan Usaha Milik Daerah) yang dimiliki oleh Pemerintah Kota Surabaya. Dalam memberikan pelayanan kepada pelanggan tentunya memerlukan Teknologi Informasi dan Sistem Informasi yang cukup memadai guna mendukung pelayanan prima kepada pelanggan, lebih-lebih di era digitalisasi saat ini. Untuk mengukur sejauh mana kemampuan PDAM Surya Sembada Kota Surabaya dalam hal tata kelola keamanan informasi maka perlu dilakukannya sebuah evaluasi tata kelola keamanan informasi. Tujuan penelitian ini adalah untuk mengetahui tingkat kematangan (*Maturity Level*) keamanan informasi, serta memberikan rekomendasi pada PDAM Surya Sembada Kota Surabaya berdasarkan evaluasi tersebut. Penelitian ini menggunakan metode skala *Systems Security Engineering Capability Maturity Model* (SSE-CMM). Perhitungan *Maturity Level* menggunakan 4 klausul yang telah ditentukan berdasarkan pada ISO/IEC 27001:2013 dan menggunakan skala *Systems Security Engineering Capability Maturity Model* (SSE-CMM). Hasil rata-rata nilai *Maturity Level* dari keseluruhan klausul sebesar 3,5 dan berada dalam *level* tiga yang mana merupakan kategori *Well Defined* artinya kinerja pada *level* ini dilakukan sesuai dengan persetujuan, sesuai dengan standar yang telah ada, dan proses telah didokumentasikan, direncanakan dan dikelola dengan menggunakan standar yang ditetapkan organisasi. Selain itu, penulis menemukan beberapa gap antara kondisi sebenarnya dengan standar ISO/IEC 27001:2013 dan telah diberikan rekomendasi. Hasil penelitian ini dapat bermanfaat sebagai bahan pertimbangan untuk memperbaiki gap yang ada sesuai dengan standar ISO/IEC 27001:2013. Sehingga kedepannya dapat digunakan sebagai dasar mengambil penilaian dan kebijakan manajemen PDAM Surya Sembada Kota Surabaya dalam penerapan Sistem Manajemen Keamanan Informasi (SMKI) sesuai standar ISO/IEC 27001: 2013.**

***Kata Kunci*—ISO/IEC 27001:2013, Keamanan Informasi, Tingkat Kematangan.**

I. PENDAHULUAN

PADA era sekarang teknologi informasi (TI) sudah merupakan bagian yang memegang peranan penting di dunia industri. Beberapa macam kemudahan diberikan oleh teknologi informasi dalam menyelesaikan berbagai masalah yang dimiliki oleh setiap individu manusia di bidang industri. Namun, di sisi lain untuk membangun sebuah infrastruktur teknologi informasi yang handal memerlukan biaya yang tidak sedikit untuk membangunnya. Teknologi informasi dalam sektor perusahaan publik dan privat, administrasi publik dan bagian lain sangat rentan sekali dari berbagai ancaman siber, seperti misalnya *virus*, serangan *hacking* pada kegagalan sistem. Untuk itu Pentingnya nilai dari sebuah informasi menyebabkan informasi seringkali hanya boleh diakses oleh orang-orang tertentu saja yang sudah memiliki hak akses yang sudah ditentukan oleh administrator. Jatuhnya informasi ke tangan pihak lain yang tidak memiliki hak akses yang telah ditentukan oleh administrator akan menimbulkan dampak yang merugikan bagi pemilik informasi tersebut, oleh karena itu keamanan sistem informasi yang akan digunakan harus terjamin dalam batas yang sudah ditentukan atau batas yang dapat diterima.

Pemilihan PDAM Surya Sembada Kota Surabaya untuk penelitian ini didasari oleh sebuah kenyataan bahwasanya menurut informasi yang didapat oleh penulis pada sekitar bulan Oktober 2021 telah terjadi *hacking* pada *Data Center* PDAM Surya Sembada yang mengakibatkan sebagian data-data perusahaan hilang sehingga dengan segala daya upaya bagian IT melakukan beberapa langkah *recovery data*, untuk menyelamatkan data-data perusahaan yang telah dicuri oleh *hacker*. Menurut informasi yang telah didapat penulis, bahwa PDAM Surya Sembada Kota Surabaya belum memiliki kebijakan manajemen yang mengatur tentang keamanan informasi. Berangkat dari permasalahan tersebut, hal yang paling penting harus diketahui adalah posisi *level* kematangan PDAM Surya Sembada Kota Surabaya dalam hal keamanan informasi. Salah satu metode penelitian yang akan digunakan untuk melakukan evaluasi tata kelola keamanan informasi PDAM Surya Sembada Kota Surabaya adalah dengan menggunakan metode berdasarkan standar ISO/IEC 27001:2013.

II. DASAR TEORI

Bagian ini menjelaskan teori-teori yang mendukung pengerjaan tugas akhir.

A. Evaluasi

Definisi evaluasi dapat dijabarkan dengan secara bahasa ataupun secara harfiah. Definisi secara bahasa, kata evaluasi berasal dari kata bahasa inggris yaitu "*evaluation*" yang memiliki arti penaksiran atau penilaian. Sedangkan definisi

Tabel 1.
Klausul ISO/IEC 27001:2013.

Klausul	Objektif Kontrol
A.5. Kebijakan Keamanan Informasi	A.5.1 Arahan Manajemen Untuk Keamanan Informasi
A.6. Organisasi Keamanan Informasi	A.6.1 Organisasi Internal
	A.6.2 Perangkat Seluler Dan *Teleworking*
A.7. Keamanan Sumber Daya Manusia	A.7.1 Sebelum Bekerja
	A.7.2 Selama Bekerja
	A.7.3 Pemutusan Hubungan Kerja Dan Perubahan Pekerjaan
A.8. Manajemen Aset	A.8.1 Tanggung Jawab Untuk Aset
	A.8.2 Klasifikasi Informasi
	A.8.3 Penanganan Media
A.9. Kontrol Akses	A.9.1 Persyaratan Bisnis Terhadap Kontrol Akses
	A.9.2 Manajemen Akses *User*
	A.9.3 Tanggung Jawab Pengguna
	A.9.4 Kontrol Akses Sistem Dan Aplikasi
A.10. Kriptografi	A.10.1 Kontrol Kriptografi
A.11. Keamanan Fisik Dan Lingkungan	A.11.1 Area Aman
	A.11.2 Peralatan
A.12. Keamanan Operasi	A.12.1 Prosedur Dan Tanggung Jawab Operasional
	A.12.2 Perlindungan Dari *Malware*
	A.12.3 *Backup*
	A.12.4 Pencatatan Dan Pemantauan
	A.12.5 Kontrol Perangkat Lunak Operasional
	A.12.6 Pengelolaan Kerentanan Teknis
	A.12.7 Pertimbangan Audit Sistem Informasi
A.13. Keamanan Komunikasi	A.13.1 Manajemen Keamanan Jaringan
	A.13.2 Transfer Informasi
A.14. Akuisisi Sistem, Pengembangan, Dan Pemeliharaan	A.14.1 Persyaratan Keamanan Sistem Informasi
	A.14.2 Keamanan Dalam Proses Pengembangan Dan Dukungan
	A.14.3 Uji Data
A.15. Hubungan Pemasok	A.15.1 Keamanan Informasi Dalam Hubungan Pemasok
	A.15.2 Manajemen Pengiriman Layanan Pemasok
A.16. Manajemen Insiden Keamanan Informasi	A.16.1 Manajemen Insiden Keamanan Informasi Dan Perbaikan

Tabel 2.
Pemilihan Objektif Kontrol Dan Kontrol Keamanan.

Klausul	Objektif Kontrol	Kontrol Keamanan
A.9. Kontrol Akses	A.9.1 Persyaratan Bisnis Terhadap Kontrol Akses	A.9.1.1 Kebijakan Kontrol Akses
		A.9.1.2 Akses ke jaringan dan layanan jaringan
A.11. Keamanan Fisik dan Lingkungan	A.11.1 Area Aman	A.11.1.2 Kontrol Entri Fisik
		A.11.1.3 Mengamankan kantor, ruangan, dan fasilitas
		A.11.1.4 Melindungi Terhadap Ancaman Eksternal dan Lingkungan
	A.11.2 Peralatan	A.11.2.2 Utilitas Pendukung
		A.11.2.3 Keamanan Kabel
		A.11.2.4 Pemeliharaan Peralatan
A.12 Keamanan Operasi	A.12.2 Perlindungan dari *Malware*	A.12.2.1 Kontrol terhadap *Malware*
	A.12.3 *Backup*	A.12.3.1 *Backup* Informasi
A.16. Pengelolaan Insiden Keamanan Informasi	A.16.1 Manajemen Insiden Keamanan Informasi dan Perbaikan	A.16.1.2 Pelaporan Peristiwa keamanan informasi
		A.16.1.3 Pelaporan kelemahan keamanan informasi
		A.16.1.4 Penilaian dan keputusan tentang kejadian keamanan informasi
		A.16.1.5 Respon terhadap insiden keamanan informasi
		A.16.1.6 Belajar dari Insiden Keamanan Informasi
		A.9.1.1 Kebijakan Kontrol Akses

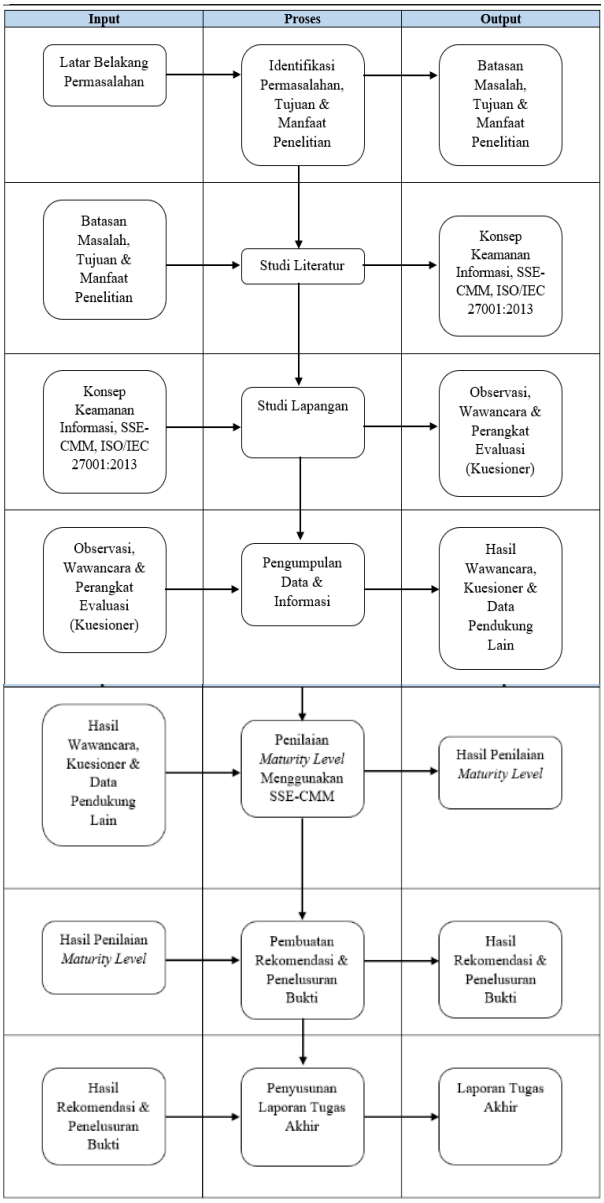
secara harfiah, evaluasi adalah proses untuk menentukan nilai suatu hal atau objek beracuan tertentu untuk dapat menggapai tujuan tertentu. Evaluasi adalah sebuah kegiatan untuk menghimpun informasi mengenai tentang kinerja sesuatu (metode, manusia, peralatan), informasi tersebut akan dipergunakan dalam menentukan alternatif terbaik dalam membuat keputusan.

B. Keamanan Informasi

Keamanan informasi memberikan perlindungan terhadap informasi dari 3 aspek keamanan informasi, yaitu *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan), dan juga memberikan perlindungan terhadap sistem serta perangkat keras yang digunakan untuk menyimpan atau mentransmisi informasi tersebut melalui penerapan kebijakan, program pelatihan dan penyadaran serta teknologi [1].

C. Tujuan Keamanan Informasi

Tiap-tiap organisasi atau perusahaan mengenakan sistem informasi berbasis komputer guna meraih tujuan tertentu. Oleh karenanya perusahaan dituntut untuk membuat sistem keamanan untuk mengamankan aset yang dimilikinya yakni berupa *hardware* dan *software* dari sistem informasi tersebut. Memiliki tujuan untuk meyakinkan kerahasiaan, ketersediaan, dan integritas dari pengolahan data. Biaya yang akan dikeluarkan oleh perusahaan untuk melakukan pengamanan terhadap sistem komputer tentunya harus wajar jika mempunyai keinginan untuk meminimalkan seminimal mungkin dari risiko-risiko dan memelihara keamanan sistem komputerisasi di suatu tingkat atau *level* yang dapat diterima. Karenanya masyarakat akan menilai reputasi organisasi dari tiga aspek di atas yakni integritas, kerahasiaan, dan ketersediaan informasi [2].



Gambar 1. Diagram metodologi penelitian.

D. Aspek Keamanan Informasi

Aspek keamanan informasi dari organisasi memiliki keharusan untuk dikontrol, diperhatikan dan di implementasi. Untuk memenuhi semua aspek keamanan informasi dilakukan dengan bertujuan untuk memberikan perlindungan pada informasi. Aspek-aspek yang berkaitan dengan *user* pada keamanan informasi, adalah *privacy*, *identification*, *authentication*, *authorization*, *accountability* [3]. Keamanan informasi juga mempunyai tiga pilar untuk mendukungnya, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*), tujuan keamanan informasi juga merupakan kerahasiaan, integritas dan ketersediaan [1].

E. Framework Keamanan Tata Kelola TI

Bahwasanya tersedia 11 kontrol penting tata kelola keamanan teknologi informasi yang harus diterapkan oleh sebuah organisasi dalam melakukan pengukuran atau evaluasi. Adapun 11 kontrol penting dalam tata Kelola keamanan teknologi informasi adalah sebagai berikut [4]: *Information Security Policy*, *Communication & Operations Management*, *Access Control*, *Information System Acquisition*, *Development and Maintenance*, *Organization of Information Security*, *Asset Management*, *Information Security Incident Management*, *Business Continuity Incident Management*, *Human Resources Security*, *Physical and Environment Security*, *Compliance*.

Tabel 3.
Level Kemampuan SSE-CMM.

Tingkat Kemampuan	Deskripsi
1	*Performed Informally* (Dilakukan Informal)
2	*Planned and Tracked* (Direncanakan dan Dilacak)
3	*Well Defined* (Didefinisikan dengan Baik)
4	*Quantitatively Controlled* (Dikendalikan secara kuantitatif)
5	*Continuously Improving* (Ditingkatkan terus-menerus)

Tabel 4.
Tujuan Wawancara.

Tujuan	Narasumber
Mengetahui kondisi terkini perusahaan terkait dengan keamanan informasi	Nasrul Amir
Mengetahui gambaran umum perusahaan serta tugas pokok dan fungsi bagian TSI	Nasrul Amir

Tabel 5.
Daftar Pelaksanaan Wawancara.

No	Hari/Tanggal	Tempat	Narasumber	Jabatan
1	Selasa, 5 April 2022	Ruang Bagian Teknologi Sistem Informasi (TSI)	Nasrul Amir	Manajer TSI
2	Rabu, 6 April 2022	Ruang SOCC (*Service and Operation Command Center*)	Nasrul Amir	Manajer TSI

F. ISO/IEC 27001 & ISO/IEC 27001:2013

ISO/IEC 27001 adalah salah satu seri yang diterbitkan oleh The International Organization for Standarization yang dalamnya berisi tentang spesifikasi atau syarat yang harus dipenuhi untuk membangun Sistem Manajemen Keamanan Informasi (SMKI) [5].

ISO/IEC 27001:2013 adalah standar versi yang paling baru dari standar ISO seri 27001 yang dirilis oleh The International Organization for Standarization pada waktu tahun 2013. Standar ISO/IEC 27001:2013 ini menyediakan persyaratan-persyaratan yang dapat dipergunakan untuk menetapkan, mengimplementasi, mempertahankan serta terus meningkatkan sistem manajemen keamanan informasi (SMKI) di suatu organisasi. Pengangkatan sebuah sistem manajemen keamanan informasi ini merupakan keputusan yang sangat strategis oleh organisasi yang tentunya telah berdasarkan oleh adanya kebutuhan dan tujuan organisasi, persyaratan keamanan, dan struktur organisasi yang tentunya akan dapat berubah seiring mengikuti perkembangan waktu [6].

G. Klausul ISO/IEC 27001:2013

Pada standar ISO/IEC 27001:2013 mempunyai 14 klausul, 35 objektif kontrol dan 144 kontrol keamanan [6] yang ditampilkan pada Tabel 1.

H. Model PDCA (Plan-Do-Check-Act)

Model ini merupakan model yang dipergunakan dalam

Tabel 6.
Pemetaan Responden Dengan Kontrol Keamanan ISO/IEC 27001:2013.

No.	Nama Responden	Jabatan	Kontrol Keamanan ISO/IEC 27001:2013
1.	Eko Yudha Prasetya	*Supervisor* Pengembangan Teknologi Informasi	A.9.1.1 Kebijakan Kontrol Akses A.12.3.1 *Backup* Informasi
2.	Dedy Purwanto	*Supervisor* Infrastruktur	A.9.1.2 Akses ke Jaringan dan Layanan Jaringan A.11.1.2 Kontrol Entri Fisik A.11.1.3 Mengamankan Kantor, Ruangan, dan Fasilitas A.11.1.4 Melindungi Terhadap Ancaman Eksternal dan Lingkungan A.11.2.2 Utilitas Pendukung A.11.2.3 Keamanan Kabel A.11.2.4 Pemeliharaan Peralatan
3.	Ira Nuraini	*Supervisor* Sistem Informasi	A.12.2.1 Kontrol Terhadap *Malware* A.16.1.2 Pelaporan Peristiwa Keamanan Informasi A.16.1.3 Pelaporan Kelemahan Keamanan Informasi A.16.1.4 Penilaian dan Keputusan tentang Kejadian Keamanan Informasi A.16.1.5 Respon Terhadap Insiden Keamanan Informasi A.16.1.6 Belajar dari Insiden Keamanan Informasi

Tabel 7.
Contoh Kerangka Kerja Perhitungan Maturity Level.

A.16	Manajemen Insiden Keamanan Informasi
A.16.1	Manajemen Insiden Keamanan Informasi dan Perbaikan
A.16.1.3	Pelaporan Kelemahan Keamanan Informasi
Kontrol: Karyawan dan kontraktor yang menggunakan sistem informasi dan layanan organisasi harus diminta untuk mencatat dan melaporkan setiap kelemahan keamanan sistem atau layanan yang diamati atau dicurigai	

No	Pernyataan	Bobot	Tingkat Kemampuan					Nilai
			1	2	3	4	5	
1.	Terdapat arahan bagi karyawan maupun kontraktor untuk mencatat kelemahan keamanan sistem yang dicurigai	1				✓		4
2.	Terdapat mekanisme pelaporan kelemahan keamanan informasi yang mudah diakses	1				✓		4
	Total Bobot	2						4,00

Tabel 8.
Contoh Hasil Perhitungan Maturity Level Klausul A.16 Manajemen Insiden Keamanan Informasi.

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
A.16 Manajemen Insiden Keamanan Informasi	A.16.1 Manajemen Insiden Keamanan Informasi dan Perbaikan	A.16.1.2 Pelaporan Peristiwa Keamanan Informasi	4,00	4,06
		A.16.1.3 Pelaporan Kelemahan Keamanan Informasi	4,00	
		A.16.1.4 Penilaian dan Keputusan tentang Kejadian Keamanan Informasi	3,00	
		A.16.1.5 Respon Terhadap Insiden Keamanan Informasi	4,33	
		A.16.1.6 Belajar Dari Insiden Keamanan Informasi	5,00	
		Maturity Level Klausul A.16		4,06

penerapan sistem manajemen keamanan informasi atau dapat disebut juga sebagai siklus SMKI. Model PDCA dirancang untuk mendorong perbaikan yang berkelanjutan. Dan menerapkan SMKI sebagaimana yang telah ditentukan dalam standar ISO/IEC 27001:2013, sebuah organisasi dapat menggunakan model PDCA [7]. Sistem Manajemen Keamanan Informasi (SMKI) dengan model *Plan*, *Do*, *Check* dan *Act* (PDCA) yang digunakan dalam penelitian evaluasi tata kelola keamanan informasi ini adalah tahapan *Check* dan *Act*

I. Systems Security Engineering Capability Maturity Model (SSE-CMM)

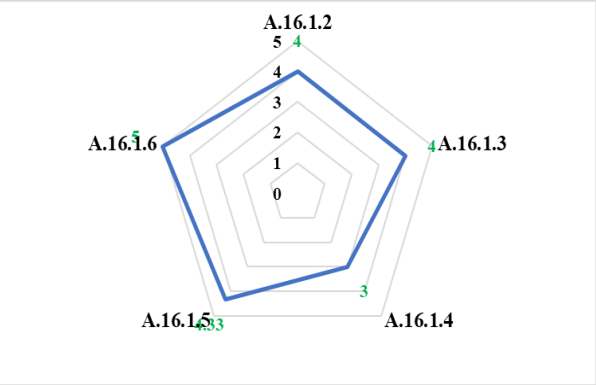
SSE-CMM adalah gambaran referensi proses yang memiliki fokus pada persyaratan guna mengimplementasikan keamanan dalam serangkaian sistem terkait yang merupakan domain keamanan teknologi informasi. SSE-CMM mempromosikan integrasi tersebut, mengambil pandangan bahwa keamanan tersebar di semua ilmu teknik. Model ini pertama kali dikembangkan oleh Carnegie Mellon University pada tahun 1995. Saat ini versi SSE-CMM yang terbaru adalah Versi 3 yang dirilis pada tahun 2003 [8].

J. Level Capability SSE-CMM (Systems Security Engineering Capability Maturity Model)

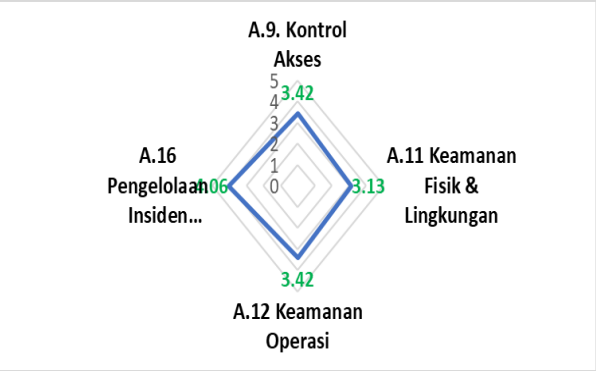
Penilaian harus dilakukan untuk menentukan tingkat kemampuan masing-masing daerah proses. Hal ini menunjukkan bahwa area proses yang berbeda dapat dan mungkin akan ada pada berbagai tingkat kemampuan. Organisasi kemudian akan dapat menggunakan informasi-informasi tertentu ini sebagai sarana untuk fokus perbaikan prosesnya. Prioritas dan urutan kegiatan organisasi untuk meningkatkan proses yang harus memperhitungkan tujuan bisnisnya [9]. *Level capability* SSE-CMM (*System Security Engineering Capability Maturity Model*) memiliki 5 tingkat dalam SSE-CMM yaitu: Level 1 "*Performed Informally*", Level 2 "*Planned and Tracked*", Level 3 "*Well Defined*", Level 4 "*Quantitatively Controlled*", Level 5 "*Continuously Improving*" [10].

K. Perhitungan Maturity Level

Nilai *Maturity Level* didapatkan dari rata-rata seluruh kontrol keamanan yang telah dihitung level kemampuannya. Setiap klausul memiliki beberapa objektif kontrol, dan setiap objektif kontrol memiliki beberapa kontrol keamanan



Gambar 2. Contoh representasi nilai *maturity level* klausul A.16 manajemen insiden keamanan informasi.



Gambar 3. Representasi nilai *maturity level* seluruh klausul.

informasi dan rata-rata yang dari kontrol keamanan itulah yang diambil untuk menghasilkan nilai *Maturity Level* setiap objektif kontrol. Sedangkan nilai *Maturity Level* tiap klausul diambil berdasarkan rata-rata objektif kontrol yang digunakan yang pada klausul tersebut. Dalam penelitian ini pembedaan istilah antara nilai kematangan dan tingkat kematangan. Nilai kematangan dapat bernilai tidak bulat (desimal), yang mempresentasikan proses pencapaian menuju suatu tingkat kapabilitas tertentu. Sedangkan tingkat kapabilitas lebih menunjukkan tahapan atau kelas yang dicapai dalam proses kapabilitas yang dinyatakan dalam bilangan bulat [9].

III. METODOLOGI

A. Diagram Metodologi

Pada sub bab ini akan dijelaskan mengenai tahapan yang dilakukan dalam penelitian sesuai, dapat dilihat pada Gambar 1.

B. Uraian Metodologi

1) Identifikasi Masalah

Pada tahap ini akan dilakukan kegiatan mencari permasalahan yang ada. Setelah permasalahan ditemukan, langkah selanjutnya adalah mencari solusi yang dapat digunakan untuk menyelesaikan permasalahan tersebut. Hasil dari tahap ini merupakan permasalahan dan usulan solusi yang dapat diangkat menjadi topik tugas akhir.

2) Studi Literatur

Pada tahapan ini akan dilakukan mencari referensi teori yang relevan dengan kasus atau penemuan permasalahan yang akan menunjang kelancaran proses pengerjaan tugas akhir. Pencarian data dan informasi dari buku, jurnal, maupun laporan penelitian yang sebelumnya dan berkaitan mengenai keamanan informasi, cara pengukurannya, dan variabel yang digunakan. Selain itu, dilakukan pencarian informasi mengenai klausul-klausul dalam ISO/IEC 27001:2013 dan Analisa tingkat kematangan (*Level Maturity*) keamanan informasi dengan menggunakan metode/indeks SSE-CMM. Dari tahap ini, penulis juga mulai menyusun instrumen penelitian berupa kuesioner yang akan digunakan dalam penelitian.

Tabel 9.
Hasil Perhitungan Nilai Maturity Level Seluruh Klausul.

Klausul	*Maturity Level*
A.9 Kontrol Akses	3,42
A.11 Keamanan Fisik dan Lingkungan	3,13
A.12 Keamanan Operasi	3,42
A.16 Manajemen Insiden Keamanan Informasi	4,06
Nilai *Maturity Level*	3,50 (*Well Defined*)

3) Pengumpulan Data dan Informasi

Pada tahap ini dilakukan pengumpulan data dan informasi yang berkaitan dengan pengerjaan tugas akhir. Penulis membutuhkan data serta informasi yang lengkap sebagai bahan untuk mendukung teori-teori yang telah dijelaskan pada Bab sebelumnya, metode pengumpulan data yang digunakan mencakup studi pustaka, studi lapangan yang terdiri dari observasi, wawancara, dan kuesioner, serta studi literatur sejenis.

4) Studi Lapangan

Studi lapangan dilakukan penulis secara langsung di Kantor Pusat PDAM Surya Sembada Kota Surabaya yang berada pada Jl. Mayjend. Prof. Dr. Moestopo No. 2 Surabaya. Studi lapangan merupakan studi yang dilakukan secara langsung ke tempat penelitian yang sudah ditentukan penulis. Studi lapangan ini antara lain meliputi:

a. Observasi

Metode observasi yang dilakukan penulis pada penelitian tugas akhir ini dengan pengamatan secara langsung di Kantor Pusat PDAM Surya Sembada Kota Surabaya Bagian Teknologi Sistem Informasi (TSI), dengan melihat proses sistem keamanan informasi dan proses untuk mendapatkan data yang dibutuhkan pada bagian Teknologi Sistem Informasi (TSI). Kegiatan observasi ini dimulai pada bulan Maret sampai dengan bulan April 2022.

b. Wawancara

Wawancara tergolong ke dalam metode pengumpulan data kualitatif. Dalam penelitian ini penulis melakukan wawancara secara langsung terhadap pejabat di bagian Teknologi Sistem Informasi pada PDAM Surya Sembada Kota Surabaya.

c. Kuesioner

Dalam penelitian ini kuesioner termasuk ke dalam metode pengumpulan data kualitatif. Dalam melakukan pengumpulan data dan penyebaran kuesioner penulis melakukan pada bagian Teknologi dan Sistem Informasi di PDAM Surya Sembada Kota Surabaya. Pertanyaan atau pernyataan pada kuesioner yang telah ditetapkan memiliki acuan pada klausul-klausul yang dipilih penulis pada standar ISO/IEC 27001:2013. Selanjutnya akan dilakukan Analisa tingkat kematangan (*Level Maturity*) keamanan informasi.

Tabel 10.
Contoh Penelusuran Bukti.

A.16	Manajemen Insiden Keamanan Informasi				
A.16.1	Manajemen Insiden Keamanan Informasi dan Perbaikan				
A.16.1.3	Pelaporan Kelemahan Keamanan Informasi				
Kontrol: Karyawan dan kontraktor yang menggunakan sistem informasi dan layanan organisasi harus diminta untuk mencatat dan melaporkan setiap kelemahan keamanan sistem atau layanan yang diamati atau dicurigai					
No	Pertanyaan	Dilakukan		Bukti	*Gap*
		Ya	Tidak		
1.	Apakah terdapat arahan bagi karyawan maupun kontraktor untuk mencatat kelemahan keamanan sistem yang dicurigai	✓	✓	Adanya *training* mengenai kesadaran akan sistem manajemen keamanan informasi (SMKI) untuk mencatat kelemahan keamanan sistem yang dicurigai	-
2.	Apakah terdapat mekanisme pelaporan kelemahan keamanan informasi yang mudah diakses	✓	✓	Terdapat SOP penanganan insiden keamanan informasi (SOP-TIF-22) yang berisi panduan dalam menentukan Langkah-langkah penanganan untuk mencegah berulangnya suatu insiden dikemudian hari, dan memastikan penanggulangan insiden dapat berjalan sesuai rencana dan IT *support* untuk pelaporan kelemahan pada keamanan informasi	-

Tabel 11.
Rekomendasi.

A.16	Manajemen Insiden Keamanan Informasi
A.16.1	Manajemen Insiden Keamanan Informasi dan Perbaikan
A.16.1.3	Pelaporan Kelemahan Keamanan Informasi
Rekomendasi	
- Berkaitan dengan kontrol A.11.1.3 sebaiknya pengelola memberikan petunjuk berupa tanda yang menerangkan bahwa terdapat tempat pengelolaan dan pengolahan data / informasi	
A.11	Keamanan Fisik dan Lingkungan
A.11.2	Peralatan
A.11.2.2	Utilitas Pendukung
Rekomendasi	
- Utilitas pendukung harus dinilai secara teratur untuk memastikan utilitas pendukung tersebut masih layak atau tidak	
A.12	Keamanan Operasi
A.12.2	Perlindungan dari *Malware*
A.12.2.1	Kontrol Terhadap *Malware*
Rekomendasi	
- Adanya peninjauan rutin terhadap *software* yang digunakan untuk memastikan *software* yang digunakan tersebut memang digunakan untuk mendukung kegiatan - Membuat peraturan tentang penggunaan perangkat lunak yang resmi karena masih ada beberapa komputer yang memakai perangkat lunak tidak resmi. - Membuat peraturan tentang *website* mana saja yang dapat digunakan apabila ingin men-*download software*	
A.16	Manajemen Insiden Keamanan Informasi
A.16.1	Manajemen Insiden Keamanan Informasi dan Perbaikan
A.16.1.4	Penilaian dan Keputusan tentang Kejadian Keamanan Informasi
Rekomendasi	
- Menyediakan dokumen klasifikasi insiden apa saja yang menjadi prioritas utama	

Pelaksanaan kuesioner dilakukan pada tanggal 7 April 2022 s/d 11 April 2022.

5) Menentukan Ruang Lingkup SMKI

Dalam melakukan pengumpulan data untuk menentukan ruang lingkup SMKI diperlukan hal-hal, sebagai berikut:

a. Mempelajari karakteristik dari PDAM Surya Sembada Kota Surabaya dimulai dari profil perusahaan, visi dan misi perusahaan serta tujuan yang ingin dicapai oleh PDAM Surya Sembada Kota Surabaya.
b. Menghimpun informasi berkaitan dengan teknologi informasi serta teknologi apa saja yang dimiliki oleh PDAM Surya Sembada Kota Surabaya yang berupa informasi *database* dan infrastruktur lainnya.

6) Pemilihan Objektif Kontrol dan Kontrol Keamanan Berdasarkan ISO/IEC 27001:2013

Memilih objektif kontrol dan kontrol keamanan informasi yang akan diimplementasikan di PDAM Surya Sembada Kota Surabaya. Selanjutnya melakukan Pemetaan ISO/IEC 27001:2013 yang akan digunakan dalam Penelitian pda Tabel 2.

7) Penilaian Maturity Level Menggunakan SSE-CMM

Dalam penilaian *Maturity Level*, penulis menggunakan *System Security Engineering Capability Maturity Model* (SSE-CMM). Langkah-langkah yang dilakukan sebelum melakukan penilaian *Maturity Level* adalah sebagai berikut:

a. Pembuatan Pernyataan

Setelah menentukan objektif kontrol dan kontrol keamanan informasi apa saja yang akan diimplementasikan, selanjutnya penulis membuat pernyataan berdasarkan kontrol keamanan dari setiap objektif kontrol yang dipilih untuk diimplementasikan di PDAM Surya Sembada Kota Surabaya. Pernyataan ini dibuat dan disesuaikan dengan berdasarkan standar ISO/IEC 27001:2013 yang memiliki isi panduan implementasi dari tiap kontrol keamanan yang dipilih.

b. Penentuan Nilai Tingkat Kemampuan (Capability Level)

Untuk menilai level kemampuan keamanan pada tiap pernyataan digunakan model *System Security Engineering Capability Maturity Model* (SSE-CMM) pda Tabel 3.

c. Perhitungan Tingkat Kematangan (Maturity Level)

Nilai *Maturity Level* bisa diperoleh dari rata-rata seluruh

kontrol keamanan yang telah dihitung sebelumnya pada level kemampuannya. Setiap klausul memiliki beberapa objektif kontrol, dan setiap objektif kontrol memiliki beberapa kontrol keamanan informasi dan rata-rata yang diperoleh dari kontrol keamanan itulah yang diambil untuk menghasilkan nilai *Maturity Level* pada setiap objektif kontrol. Sedangkan nilai *Maturity Level* tiap klausul diambil berdasarkan rata-rata objektif kontrol yang digunakan pada klausul tersebut. Sedangkan untuk pemberian pembobotan pada setiap pernyataan kontrol keamanan, menurut Sarno dan Iffano (2009) bahwa pembobotan pada setiap pernyataan kontrol keamanan yang digunakan mengacu pada resiko yang akan terjadi. Dalam hubungannya dengan SMKI, resiko adalah dampak yang ditimbulkan atas terjadinya sesuatu yang mengancam keamanan informasi di organisasi, sehingga setiap pernyataan akan diberikan bobot sesuai dengan nilai resiko yang akan terjadi apabila tidak diterapkan [3].

8) Pemberian Rekomendasi

Tahapan ini terdiri dari tahap penelusuran bukti dan tahap pemberian rekomendasi.

a. Penelusuran Bukti

Pada tahap ini dilakukan penelusuran bukti berdasarkan hasil penilaian *Maturity Level*. Ini bertujuan untuk menyelaraskan hasil perhitungan *Maturity Level* agar sesuai dengan kondisi sebenarnya dari keamanan informasi di PDAM Surya Sembada Kota Surabaya. Serta untuk mengetahui apakah ada gap antara kondisi saat ini dengan panduan implementasi kontrol keamanan yang ada pada ISO/IEC 27001:2013, bahwa ISO/IEC 27001:2013 hanya sebagai panduan saja, tidak mengukur tingkat kematangan implementasi atau nilai gap. Untuk mengukur tingkat kematangan dipergunakan framework selain ISO/IEC 27001:2013 [6], [8].

b. Pemberian Rekomendasi

Tahap ini bertujuan untuk memberikan usulan perbaikan serta pengembangan terhadap Sistem Manajemen Keamanan Informasi di PDAM Surya Sembada Kota Surabaya. Rekomendasi yang diberikan beracuan pada standar ISO/IEC 27001:2013 yang memiliki isi panduan implementasi tiap kontrol keamanan yang ada pada ISO/IEC 27001: 2013.

IV. HASIL DAN PEMBAHASAN

A. Ruang Lingkup Sistem Manajemen Keamanan Informasi (SMKI)

Pada penelitian ini, penulis melakukan penelitian pada bagian Teknologi dan Sistem Informasi (TSI). Bagian Teknologi Sistem Informasi (TSI) dipimpin oleh Manajer Teknologi Sistem Informasi yang bertanggung jawab kepada Manajer Senior Teknologi Sistem Informasi dan Aset Properti. Manajer Teknologi Sistem Informasi membawahi:

1. *Supervisor* Infrastruktur;
2. *Supervisor* Sistem Informasi;
3. *Supervisor* Pengembangan Teknologi Informasi
4. *Supervisor* Kontrol Digital dan Instrumentasi.

B. Pengumpulan Data dan Informasi

1) Wawancara

Metode wawancara pada tahap ini memiliki peran penting dalam hal pengumpulan data yang akan membantu keberlangsungan pengerjaan tugas akhir. Kegiatan wawancara dilaksanakan dengan melakukan tanya jawab secara langsung kepada Manajer Teknologi Sistem Informasi (TSI) PDAM Surya Sembada Kota Surabaya di Kantor Pusat PDAM Surya Sembada Kota Surabaya yang ditampilkan pada Tabel 4 dan Tabel 5.

2) Pemetaan Responden

Untuk pelaksanaan pengisian pernyataan dan pertanyaan dalam kuesioner, penulis melakukan pemetaan responden yang dilakukan bersama dengan Manajer Teknologi Sistem Informasi (TSI) hal tersebut bertujuan agar pernyataan dan pertanyaan tiap klausul ISO/IEC 27001:2013, dijawab tepat sasaran sesuai dengan tupoksi pengelolaan keamanan sistem informasi pada PDAM Surya Sembada Kota Surabaya. Hasil pemetaan responden tersebut ditampilkan pada Tabel 6.

C. Penilaian Maturity Level Menggunakan SSE-CMM (System Security Engineering Capability Maturity Level)

Tahap ini merupakan tahap untuk menggambarkan sudah sejauh mana PDAM Surya Sembada Kota Surabaya dapat memenuhi proses pengelolaan keamanan informasi berdasarkan standar ISO/IEC 27001:2013 dan dilakukan terhadap masing-masing kontrol keamanan. Daftar pernyataan yang penulis gunakan di dalam penelitian ini dibuat berdasarkan kontrol keamanan dari setiap objektif kontrol yang dipilih untuk melakukan evaluasi tata kelola keamanan informasi PDAM Surya Sembada Kota Surabaya. Daftar pernyataan yang penulis gunakan dibuat berdasarkan standar ISO/IEC 27001:2013 yang berisi tentang panduan implementasi dari masing-masing kontrol keamanan yang sudah diuraikan di atas. Dalam penelitian ini penulis menggunakan *System Security Engineering Capability Maturity Level* (SSE-CMM) untuk mengukur *Maturity Level* proses pengelolaan keamanan informasi berdasarkan standar ISO/IEC 27001:2013. Contoh kerangka kerjanya dapat dilihat pada Tabel 7 dan Tabel 8, dan contoh representasinnya di tampilkan pada Gambar 2 dan Gambar 3.

D. Penelusuran Bukti dan Rekomendasi

Setelah mengukur *Maturity Level* dari tiap-tiap objektif kontrol serta kontrol keamanan pada PDAM Surya Sembada Kota Surabaya, langkah selanjutnya yaitu melakukan penelusuran bukti terhadap pernyataan-pernyataan yang ada pada kontrol keamanan. Penelusuran bukti ini berguna untuk mensinkronkan / mencocokkan hasil nilai *Maturity Level* yang sudah diberikan oleh beberapa responden melalui kuesioner dengan kondisi sebenarnya yang ada pada PDAM Surya Sembada Kota Surabaya. Setelah tahap penelusuran bukti selesai dilakukan, maka langkah berikutnya adalah memberikan rekomendasi kepada PDAM Surya Sembada Kota Surabaya untuk dapat memperbaiki serta meningkatkan kontrol keamanan informasi yang sesuai dengan standar ISO/IEC 27001:2013. Hasil perhitungan nilai *Maturity Level* terdapat pada Tabel 9.

1) Penelusuran Bukti

Setelah melakukan penilaian *Maturity Level* serta merepresentasikan dalam bentuk grafik di atas, penulis melakukan penelusuran bukti terhadap dokumen yang ditampilkan pada Tabel 10.

2) Rekomendasi

Mengacu dari gap yang ada dari 4 kontrol keamanan antara lain kontrol keamanan A.11.1.3 (Mengamankan Kantor, Ruangan, dan Fasilitas), A.11.2.2 (Utilitas Pendukung), A.12.2.1 (Kontrol Terhadap *Malware*), A.16.1.4 (Penilaian dan Keputusan tentang Kejadian Keamanan Informasi), selanjutnya penulis memberikan beberapa rekomendasi. Berikut beberapa rekomendasi yang dapat penulis berikan untuk dapat memperbaiki gap yang ada pada PDAM Surya Sembada Kota Surabaya. Rekomendasi yang diberikan ditampilkan pada Tabel 11.

V. KESIMPULAN

Dari penelitian tugas akhir yang telah dilakukan, dapat diambil kesimpulan sebagai berikut: (1) Dari hasil perhitungan *Maturity Level* didapatkan hasil rata-rata dari 4 klausul ISO/IEC 27001:2013 yang digunakan adalah sebesar 3,5 yang mana hasil perhitungan *Maturity Level* tersebut menunjukkan ke dalam kategori *Well Defined* artinya kinerja pada level ini dilakukan sesuai dengan persetujuan, sesuai dengan standar yang telah ada, dan proses telah didokumentasikan, direncanakan dan dikelola dengan menggunakan standar yang ditetapkan organisasi. (2) Ditemukan beberapa gap yang ditemukan oleh penulis, diantaranya pada kontrol keamanan A.11.1.3 (Mengamankan Kantor, Ruangan, dan Fasilitas), A.11.2.2 (Utilitas Pendukung), A.12.2.1 (Kontrol Terhadap *Malware*), A.16.1.4 (Penilaian dan Keputusan tentang Kejadian Keamanan Informasi). (3) Beberapa gap yang ditemukan oleh penulis disebabkan karena adanya kegiatan pada bidang IT PDAM Surya Sembada Kota Surabaya belum memiliki peraturan dan prosedur pelaksanaan kegiatan secara tertulis dalam pengimplementasiannya. (4) Dari hasil penelitian yang telah dilakukan oleh penulis, maka diberikan suatu rekomendasi pada beberapa kontrol keamanan, seperti kontrol keamanan A.11.1.3 (Mengamankan Kantor, Ruangan, dan Fasilitas), A.11.2.2 (Utilitas Pendukung), A.12.2.1 (Kontrol Terhadap *Malware*), A.16.1.4 (Penilaian dan Keputusan tentang Kejadian Keamanan Informasi) hal tersebut di atas untuk evaluasi terhadap insiden guna mencegah terjadinya insiden serupa yang pernah terjadi.

VI. SARAN

Berdasarkan hasil penelitian pada tugas akhir ini, maka saran untuk penelitian selanjutnya adalah sebagai berikut: (1) Untuk dapat ditingkatkan dan ditekankan *core value* perusahaan yang dapat mempertahankan hasil yang telah dicapai. (2) Melakukan *monitoring* dan evaluasi tata kelola keamanan informasi untuk ditingkatkan terus menerus serta adanya proses perbaikan secara berkesinambungan untuk mencapai *maturity level* yang lebih tinggi (level 4 atau level yang paling tinggi yaitu level 5). (3) Evaluasi Tata kelola Keamanan Informasi ini menggunakan *framework* ISO 27001:2013 dan penilaian *maturity level* dengan menggunakan model SSE-CMM, maka untuk pengembangan penelitian selanjutnya disarankan dapat menggunakan penilaian *maturity level* dengan model lain, yaitu *Capability Maturity Model for Integration* (CMMI) COBIT sebagai bahan perbandingan.

DAFTAR PUSTAKA

[1] M. E. Whitman and H. J. Mattord, *Principles of Information Security*, 5th ed. Boston: Cengage Learning, 2014.

[2] IBISA and T. A. Prabawati, *Keamanan Sitem Informasi*. Yogyakarta: Andi, 2011.

[3] R. Sarno and I. Iffano, *Sistem Manajemen Keamanan Informasi (Berbasis ISO 27001)*. Surabaya: ITS Press, 2010.

[4] A. Alfantookh, *An Approach for the Assessment of the Application of ISO/IEC 27001:2013 Essential Information Security Controls*. Riyadh: King Saud University , 2009.

[5] Direktorat Keamanan Informasi, *Panduan Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks Keamanan Informasi (Indeks KAMI)*. Jakarta: Direktorat Keamanan Informasi, 2017.

[6] International Organization for Standardization, *ISO/IEC 27001:2013 Information Technology-Security-Techniques Information Security Management Systems-Requirements*, 2nd ed. Switzerland: International Organization for Standardization, 2013.

[7] S. T. Arnason and K. D. Willett, *How to Achieve 27001 Certification: An Example of Applied Compliance Management*. Florida: Auerbach Publications, 2019.

[8] Carnegie Mellon University, *A Systems Engineering Capability Maturity Model (SE-CMM)*. Pittsburgh: Carnegie Mellon University, 2003.

[9] K. Surendro, *Implementasi Tata Kelola Teknologi Informasi*. Bandung: Informatika, 2009.

[10] Carnegie Mellon University, *Systems Security Engineering Capability Maturity Model (SSE-CMM)*. Pittsburgh: Carnegie Mellon University, 2013.