p-ISSN 2088-5407
e-ISSN 2621-9001

ANALISIS SISTEM MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN SNI ISO/IEC 27001:2013 PADA PEMERINTAHAN DAERAH KOTA SUKABUMI (STUDI KASUS: DI DISKOMINFO KOTA SUKABUMI)

Winda Apriandari[#1], Ashwin Sasongko[*2]

[#]*Teknik Informatika Universitas Muhammadiyah Sukabumi*, winda.apriandari@gmail.com

[*]*Teknik Informatika Universitas Langlangbuana*, ashwin.sasongko@gmail.com

ABSTRACT

DISKOMINFO (Communication and Information Service) of Sukabumi is a government institution that has responsibility for the management of Information and Communication Technology in Local Government (PEMDA) Sukabumi. Sukabumi Information Technology managed by Head of Infrastructure of ICT, Encryption and Data Integration. From the results of interviews and observation , DISKOMINFO has problems on managing data securit, is because lack of Human Resources, lack of awareness and responsibility and implementation of poor information security that cause incidents or hacking of information security, especially in Sukabumi City Information System. this causes disruption of the process of public service and business in DISKOMINFO.The Information Security Management System (ISMS) is a management system implemented by organizations, especially governments organitations, to secure information assets against threats that exist within the scope of DISKOMINFO. The process carried out using the PDCA cycle approach among the Plan Do Check Act. The ISMS handle infomation aspects such as confidentiality, integrity, and availability information.The ISMS analysis uses SNI ISO / IEC 27001: 2013 and SNI ISO / IEC 31000: 2009 risk management base. The ISMS analysis purpose to identify risk profiles by identifying assets, threats, and vulnerabilities as well as evaluating and controlling disruptions. ISMS produce security information manual, information security procedure, work instruction and information security form.

Keywords : Information Security Management System, ISMS Analysis, SNI ISO/IEC 27001:2013, SNI ISO/IEC 31000:2009

PENDAHULUAN

1. Latar Belakang Masalah

Sistem Pemerintahan Kota Sukabumi memiliki aset terpenting sebagai sarana bagi masyarakat Kota Sukabumi, diantaranya informasi mengenai portal berita Kota tentang informasi umum Kota Sukabumi beserta arsip, infomasi dan data, Pemerintahan yang meliputi walikota, DPRD, SKPD/BUMD dan Aparatur, Investasi berupa sarana, kawasan bisnis dan UKM serta SAKIP. Dari beberapa aset tersebut, yang menjadi bagian terpenting yaitu pada keamanan informasinya. Keamanan informasi mendasari tingkatan

layanan Teknologi Informasi yang lebih baik dan menjadi salah satu faktor kelayakan teknologi.

Penulis fokus pada isu-isu keamanan layanan Teknologi Informasi. Analisis yang didapatkan penulis pada layanan komunikasi atau komplein yang disediakan dan dikendalikan oleh Kabid Infrastruktur TIK, Persandian dan Integrasi Data di Pemerintahan Daerah Kota terdapat masalah. Dikutip dalam artikel di www.tecnoid.id pada tanggal 10 April 2015 [1], "Sistem Informasi Pemerintahan Daerah Kota Sukabumi terjadi peretasan oleh pihak yang tidak berkepentingan". Pernyataan tersebut pungkas dari Bapak Wakil Wali Kota Sukabumi, Bapak Achmad Fahmi. Dari Hasil wawancara bersama narasumber Kabid Infrastruktur TIK, Persandian Dan Integrasi Data di DISKOMINFO Pemerintahan Daerah Kota Sukabumi oleh Bapak Yuli Noviawan, "Hal tersebut menyebabkan sistem *blank*, Pemerintah Daerah Kota Sukabumi mengalami kerugian 100 juta rupiah selama 1 tahun untuk memperbaiki dan perlindungan terhadap sistem yang diretas. Serangan masuk melalui layanan komunikasi atau komplein yang disediakan oleh PEMDA untuk masyarakat. Masyarakat tidak bisa memberikan komplein, saran dan mengetahui informasi yang dibutuhkan. Layanan menjadi tidak tersedia akibat sering terjadinya peretasan tersebut. Selain itu dari hasil wawancara yang didapat, DISKOMINFO memiliki kekurangan pada Sumber Daya Manusia (SDM). Sudah hampir 10 tahun belum menerima dan merekrut pegawai PNS yang baru. Sehingga dalam menangani sistem yang makro DISKOMINFO memiliki kekurangan Sumber Daya Manusia. Di bidang IT pada DISKOMINFO hanya memiliki 3 pegawai, diantaranya Bapak Yuli Noviawan, Bapak Gian dan Bapak Irfan. Dari Pemerintahan Pusat ada 3 orang sebagai tim atau relawan yang membantu dalam hal teknisi tetapi bukan dari pegawai PNS DISKOMINFO. Hal tersebut menjadi faktor kelemahan dalam penanganan dan pengelolaan sebuah sistem, dikarenakan kekurangan pegawai yang bisa menangani keamanan informasi. Dari permasalahan yang ada bahwa keamanan informasi yang baik hanya dapat dicapai melalui pembenahan aspek manajemennya.

Hasil pengamatan di DISKOMINFO kerentanan pada Teknologi Informasi disebabkan belum dilakukan kajian atau telaah terhadap risiko keamanan yang timbul, seperti sistem informasi, layanan dan sumber daya lainnya. Kajian risiko yang dimaksud identifikasi terhadap kejadian-kejadian yang mengancam kemanan informasi pada PEMDA di DISKOMINFO Kota Sukabumi dan potensi dampak kerugiannya, belum adanya analisis akibat kelemahan pada sistem yang mengalami ancaman dan peretasan dengan menggunakan kontrol tertentu.

Standar yang digunakan selain SNI ISO/IEC 27001:2013 adalah menggunakan *Capability Maturity Model Integration*

(CMMI) untuk mengukur tingkat kematangan berdasarkan klausul SNI ISO/IEC 27001:2013 dan menggunakan SNI ISO/IEC 31000:2009 untuk mengetahui profil risiko dari tahapan manajamen risiko. Klausul A.7 Keamanan Sumber Daya Manusia, A.9 Kontrol Akses, A.14 Akuisisi Pengembangan dan Pemeliharaan dipilih sesuai dengan hasil identifikasi profil risiko yang terjadi di DISKOMINFO Kota Sukabumi dan sudah ditentukan serta disepakati bersama dengan Kabid Infrastruktur TIK, Persandian Dan Integrasi Data

1. Rumusan Masalah
   a. Bagaimana menentukan ruang lingkup Analisis Sistem Manajemen Keamanan Informasi dengan menggunakan SNI ISO/IEC 27001:2013 terhadap Infrastruktur Teknologi Informasi PEMDA di DISKOMINFO Kota Sukabumi dengan mengimplementasikannya ke dalam bentuk dokumen yang berisi manual, instruksi kerja, prosedur dan formulir.
   b. Bagaimana meminimalisir keamanan informasi dengan melakukan manajemen risiko merujuk pada SNI ISO/IEC 31000:2009 untuk mengetahui profil risiko dan kontrol perlindungan keamanan terhadap Teknologi Informasi PEMDA di DISKOMINFO Kota Sukabumi.
   c. Bagaimana mengetahui kinerja suatu keamanan informasi dengan mengukur tingkat kematangan berdasarkan klausul yang dipilih yaitu Klaususl A.7 Keamanan Sumber Daya Manusia, A.9 Kontrol Akses, A.14 Akuisisi Pengembangan dan Pemeliharaan untuk mengetahui kondisi penerapan keamanan informasi PEMDA yang sedang berlangsung dan mengukur tingkat kematangan SMKI yang dibangun menggunakan *Capability Maturity Model Integration* (CMMI).
   d. Bagaimana melakukan pemeliharaan terhadap Sistem Manajemen Keamanan Informasi yang sudah diterapkan di DISKOMINFO tetapi masih terdapat kekurangan dalam menangani masalah keamanan informasi.
3. Batasan Masalah
   a. Kebutuhan ruang lingkup analisis sistem manajemen keamanan informasi dengan menggunakan model *Plan Do Check Act* (PDCA) untuk mengatur penilaian risiko, evaluasi risiko, kontrol perlindungan keamanan, desain dan manjemen keamanan dengan SNI ISO/IEC 27001:2013.
   b. Manajemen risiko menggunakan SNI ISO/IEC 31000:2009 sedangkan untuk penilaian risiko dibatasi pada aset layanan informasi, layanan

publik, komplein masyarakat dan kinerja yang ada di DISKOMINFO Kota Sukabumi dengan Sistem Manajemen Keamanan Informasi yang dibuat berdasarkan manual, instruksi kerja, prosedur dan formulir SMKI.

c. Pengukuran tingkat keamanan berdasarkan klausul yang dipilih yaitu Klaususl A.7 Keamanan Sumber Daya Manusia, A.9 Kontrol Akses, A.14 Akuisisi Pengembangan dan Pemeliharaan dengan menggunakan *Capability Maturity Model Integration* (CMMI).

d. Pemeliharaan Sistem Manajemen Keamanan Informasi di DISKOMINFO diukur menggunakan *Capability Model Maturity*

4. Tujuan Penelitian

a. Mengetahui dan menghasilkan ruang lingkup analisis sistem manajemen keamanan informasi dengan menggunakan SNI ISO/IEC 27001:2013 terhadap Infrastruktur Teknologi Informasi PEMDA di DISKOMINFO untuk rekomendasi kebijakan dalam bentuk dokumen yang berisi manual, instruksi kerja, prosedur dan formulir.

b. Untuk mengetahui ancaman apa saja yang masuk ke dalam Keamanan Informasi, mengurangi hal yang berpotensi mengganggu sistem serta mendefinisikan profil risiko dengan menggunakan SNI ISO/IEC 31000:2009 dan mendefinisikan kontrol perlindungan keamanan informasinya.

c. Untuk mendapatkan penilaian atau gap kinerja suatu keamanan informasi dari pengukuran tingkat kematangan berdasarkan klausul yang dipilih yaitu Klaususl A.7 Keamanan Sumber Daya, A.9 Kontrol Akses, A.14 Akuisisi Pengembangan dan Pemeliharaan dengan menggunakan *Capability Maturity Model Integration* (CMMI).

d. Pemeliharaan Sistem Manajemen Keamanan Informasi dengan pengukuran *Capability Maturity Model Integration* (CMMI) untuk mengidentifikasi bagian kelemahan keamanan informasi dan melakukan saran perbaikan .

METODOLOGI PENELITIAN

Metodologi penelitian memaparkan langkah-langkah yang dilakukan dan digunakan ke dalam pendekatan-pendekatan terkait dengan jenis metodologi penelitian. Di dalam jurnal menurut Leedy dan Ormrod : 2005 [12], penelitian adalah tahapan dalam mengumpulkan, menganalisis, dan menginterpretasi data untuk memahami fenomena yang terjadi. Ada beberapa jenis metodologi penelitian, diantaranya metode

deskriptif, metode kuantitatif dan metode kualitatif. Penulis menggunakan metode deskriptif dan kualitatif.

TINJAUAN DAN STUDI PUSTAKA

1. Pengertian Analisis Sistem

Analisis sistem merupakan suatu konsep yang akan dirancang oleh satu atau sekelompok orang. Analisis itu mengidentifikasi, menyatakan, merencanakan, menyusun dan merancang masalah-masalah dalam suatu objek atau sistem. Tahapan kerja dari analisis sistem sebagai berikut:

a. Mengidentifikasi masalah kebutuhan *user*
b. Melaksanakan studi kelayakan
c. Analisis dan rancang sistem
d. Penerapan sistem
e. Evaluasi dan pemeliharaan

2. Pengertian Teknologi Informasi

Teknologi merupakan kemampuan manusia yang didapat dari hasil pemikiran untuk mengembangkan sistem dalam penyelesaian persoalan dalam hidup manusia. Informasi merupakan sebuah berita yang memiliki makna, berita bisa dalam bentuk data atau pesan. Sedangkan Teknologi Informasi merupakan suatu Teknologi yang memiliki kemampuan dalam mengolah data, memanipulasi data, dan selanjutnya diproses sesuai kebutuhan untuk mendapatkan hasil yaitu sebuah informasi. Hasil informasi tersebut dapat disimpan dan diolah kembali sesuai kebutuhan.[14]

3. Pengertian Sistem Informasi

Sistem Informasi merupakan sistem yang terdapat di suatu organisasi seperti Pemerintahan yang didalamnya memiliki unsur Teknologi Informasi, proses masukan, dan hasil informasi untuk membuat sarana komunikasi bagi pengguna. Sistem Informasi memiliki komponen-komponen, diantaranya *input*, model, *output*, *technology*, dan *control*.[15]

4. Keamanan Informasi

Keamanan Informasi adalah mengamankan suatu aset yang berharga bagi kelangsungan hidup organisai baik Pemerintah maupun non Pemerintah. Aset tersebut adalah sebuah informasi. Keamanan informasi adalah hal yang harus diutamakan dan diperhatikan oleh organisasi dari tindakan kriminal yang ilegal oleh pihak yang tidak berwenang. Pertama kebocoran informasi, kedua merubah dan memanipulasi aset atau informasi, merusak sistem yang dapat menyebabkan kerugian baik dari sisi finansial maupun produktifitas organisasi. Melindungi keamanan informasi sebaik mungkin selalu ada upaya yang harus dilakukan. Keamanan informasi dalam suatu organisasi memiliki beberapa aspek-aspek, diantaranya adalah :

a. *Confidentiality* (Kerahasiaan)

Merupakan keamanan informasi yang menjamin, memastikan dan menjaga kerahasiaan aset, bahwa hanya dapat diakses oleh mereka yang memiliki wewenang.

b. *Integrity* (Integritas)

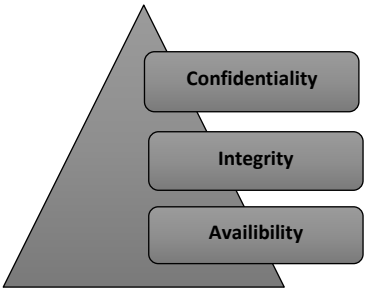
Merupakan keamanan informasi yang menjamin kelengkapan aset, menjamin aset

p-ISSN 2088-5407
e-ISSN 2621-9001

tersebut tidak berubah dan dimodifikasi maupun dihilangkan tanpa otorisasi yang tidak jelas. Menjaga keakuratan dan ancaman dari pihak luar yang tidak berkepentingan.

c. *Availibility* (Ketersediaan)

Merupakan keamanan informasi yang menjamin bahwa aet tetap tersedia, dapat diakses ketika dibutuhkan tanpa adanya gangguan dari pihak lain.



Gambar 1. Aspek Keamanan Informasi [19]

5. Ruang Lingkup/Model Keamanan Informasi

Ruang lingkup atau model keamanan informasi yang terdiri dari strategi organisasi, manusia, proses, dan teknologi. Berikut penjelasannya:

a. Strategi Organisasi

Organisasi yang memiliki pencapaian dalam menyelesaikan tujuan. Dengan membuat rancangan dari aturan atau kebijakan, proses dan arsitekturnya.

b. Manusia

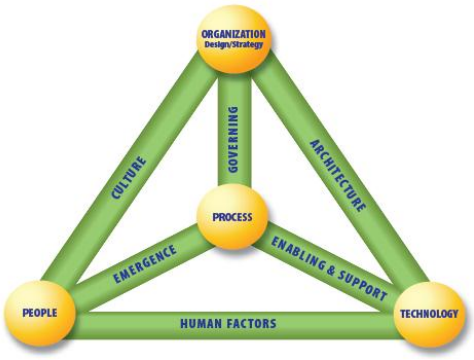
Sumber daya manusia yang memiliki tugas agar dapat dipercayai dalam menajaga aset penting organisasi.

c. Proses

Proses berasal dari kebutuhan organisasi, implementasi yang baik untuk menyelesaikan dan menyediakan kebutuhan.

d. Teknologi

Teknologi membantu organisasi untuk meningkatkan keamanan yang berasal dari perangkat keras dan lunak agar membuat proses lebih efisien.



Gambar 2. Ruang Lingkup atau Model Keamanan Informasi
(**Sumber:**https://www.isaca.org/KnowledgeCenter/PublishingImages/BMIStriangle.jpg)

6. Sistem Manajemen Keamanan Informasi

SMKI adalah suatu sasaran untuk mencapai tujuan dalam organisasi dengan menetapkan, mengimplementasikan, menggunakan, pemantauan, peninjauan, pemeliharaan dan meningkatkan keamanan informasi. Proses yang dilakukan dengan menggunakan pendekatan siklus PDCA *yaitu Plan Do Check Act*. Keamanan sistem informasi tidak hanya berhubungan dengan perangkat keras dan perangkat lunak seperti *firewall, antivirus,* penggunaan *password*

untuk komputer tetapi pendekatan terhadap sisi manusia, proses, dan teknologi serta tempat berlangsungnya pengamanan untuk menjamin keamanan dalam berjalannya efektivitas atau kegiatan.

Sistem Manajemen Keamanan Informasi diatur dalam regulasi Peraturan Menteri Komunikasi Dan Informatika Republik Indonesia nomor 4 tahun 2016 [9]. Di Bab III Standart Sistem Manajemen Keamanan Informasi di dalam pasal 7 ayat 1 menjelaskan bahwa penyelenggaraan sistem elektronik strategis harus menerapkan standart SNI ISO/IEC 27001 dan ketentuan pengamanan. Penyelenggaraan sistem elektronik diwajibkan untuk menerapkan pedoman indeks.

7. SNI ISO/IEC 27001:2013

Standar Nasional Indonesia (SNI) ISO/IEC 27001:2013 adalah standarisasi yang ruang lingkup nya dalam Sistem Manajemen Keamanan Informasi (SMKI). Standar ini dibuat khusus untuk menyediakan persyaratan untuk penetapan, penerapan, pemeliharaan dan perbaikan berkelanjutan terhadap Sistem Manajemen Keamanan Informasi (SMKI). SMKI SNI ISO/IEC 27001:2013 telah ditetapkan oleh Badan Standarisasi Nasional Nomor 61/KEP/BSN/4/2016 [20].

Struktur Organisasi ISO/IEC 27001:2013 dibagi dalam dua bagian, diantaranya:

a. Klausul : *Mandatory Process*

   Jika Organisasi menetapkan SMKI, klausul (pasal) syarat yang harus dipenuhi dengan menggunakan SNI ISO/IEC 27001:2013.

b. Annex A : *Security Control*

   Annex adalah dokumen yang disediakan dan dapat dijadikan tujuan untuk menentukan kontrol keamanan yang perlu diimplementasikan di dalam SMKI yang terdiri dari 14 klausul kontrol keamanan, 35 Objektif Kontrol dan 114 kontrol keamanan informasi.

8. SNI ISO/IEC 31000:2009

SNI ISO/IEC 31000:2009 pada klausul 5.3 di dalam SNI ISO/IEC 27001:2013 digunakan sebagai acuan untuk membangun konteks eksternal dan internal organisasi yang relevan dengan tujuan dapat mempengaruhi kemampuan untuk mencapai hasil yang diharapkan dari Sistem Manajemen Keamanan Informasi. SNI ISO/IEC 31000:2009 adalah sebuah standar internasional yang disusun dengan tujuan memberikan prinsip dan panduan untuk menerapkan manajemen risiko. Di dalam SNI ISO/IEC 31000:2009 organisasi yang menerapkan manajemen risiko perlu memperhatikan tiga aspek, diantaranya: penerapan manajemen risiko harus disertai komitmen tinggi dari pengurus organisasi (Direksi atau Komisaris), manajemen risiko harus diintegrasikan ke dalam seluruh proses organisasi dan menjadi bagian dari pemilik atau penanggung jawab proses (kepala atau staf) dan manajemen risiko harus menjadi bagian dari proses pengambilan keputusan pada tingkat *Governance*.

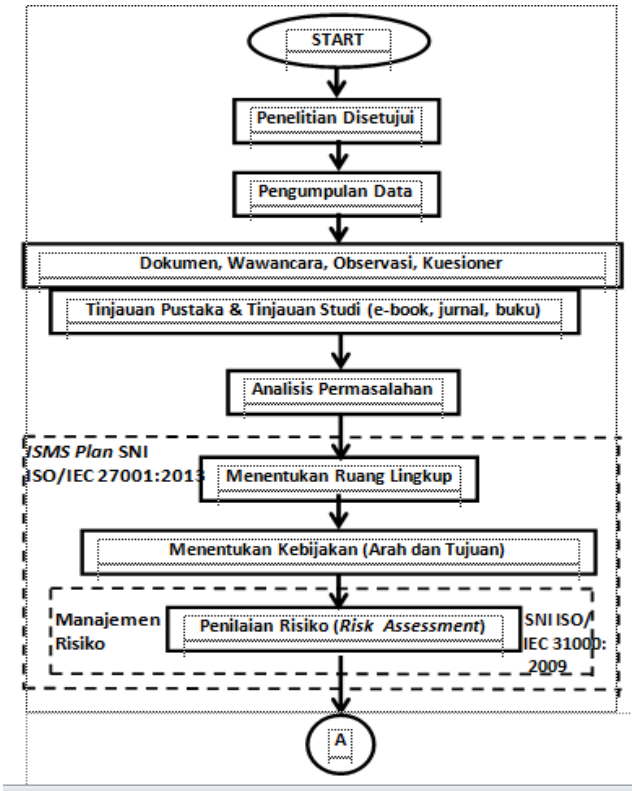
9. *Capability Model Maturity Level* (CMMI)

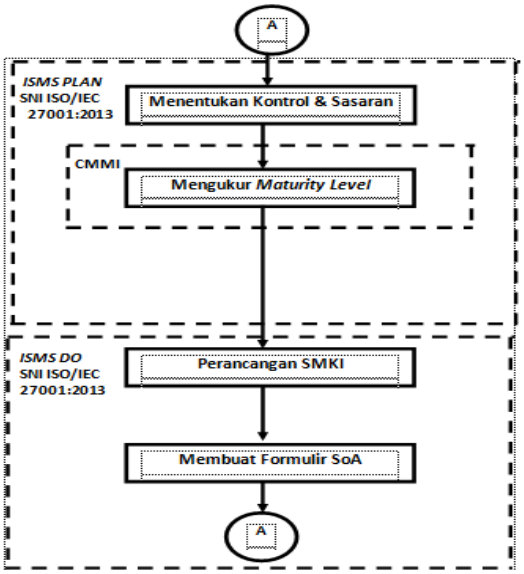
p-ISSN 2088-5407
e-ISSN 2621-9001

CMMI adalah model yang digunakan untuk pendekatan penilaian kematangan dan kemampauan organisasi. CMMI sebelumnya dikenal sebagai CMM yang diperbarahui oleh *Software Enginnering Institute* (SEI) di Carnegie Mellon University di Amerika Serikat pada akhir tahun 2001 dan di sebarkan Agustus tahun 2006.[11] CMMI dan ISO memiliki tingkat ketelitiannya yang berbeda, ISO tidak sampai mengatur jauh mengenai kebutuhan *user* sedangkan CMII selain memiliki SOP, CMII memiliki aturan yang khusus tentang SOP. Didalam CMMI terdpat *generic goals* (GG) untuk menggambarkan karakteristik di organisasi. *Generic practices* (GP) adalah *best practices* untuk mencapai GG.

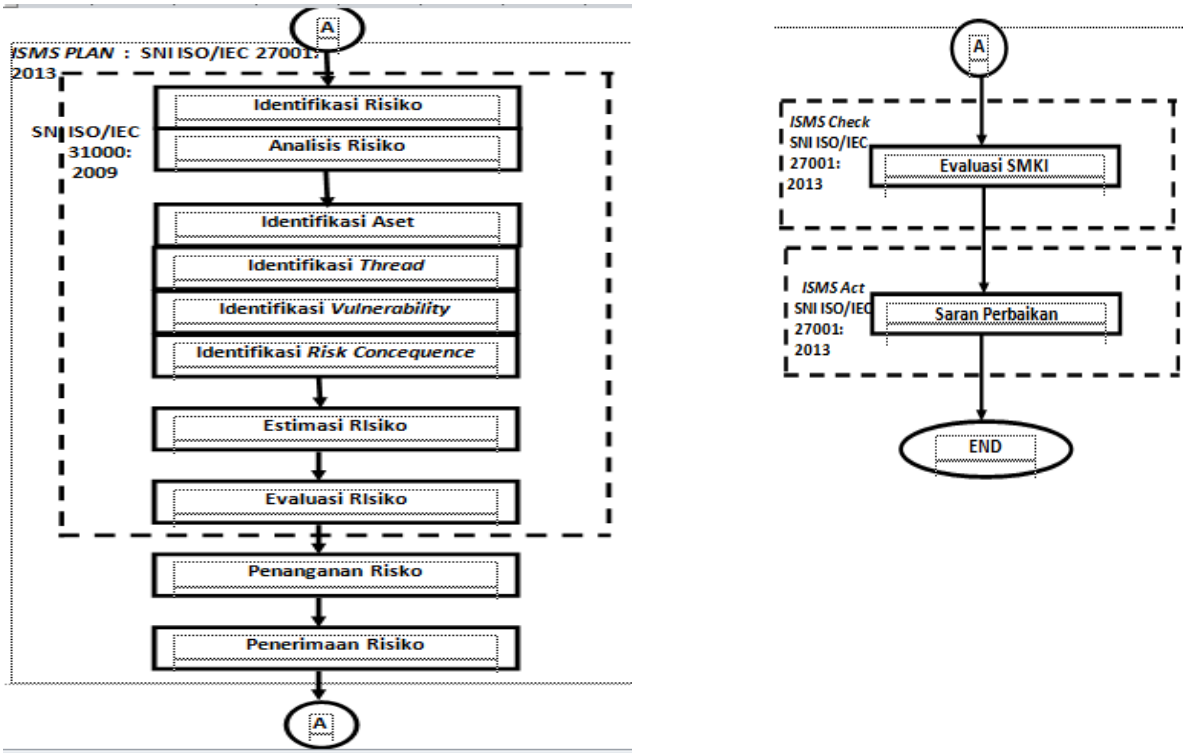
HASIL DAN PEMBAHASAN

1. Kerangka Penelitian





p-ISSN 2088-5407
e-ISSN 2621-9001



Gambar 3. Kerangka Penelitian Analisis Sistem Manajemen Keamanan Informasi

2. Manajemen Risiko Menggunakan SNI ISO/IEC 31000:2009

Di dalam SNI ISO/IEC 27001:2013 dirujuk untuk menentukan masalah eksternal dan internal yang relevan guna membangun konteks eksternal dan internal dalam klausul 5.3 SNI ISO/IEC 31000:2009. Langkah dalam memulai manajemen risiko dipaparkan sebagai berikut:

a. Penilaian Risiko (*Risk Assessment*)
   - Identifikasi Risiko (*Risk Identificstion*)
   - Analisis Risiko (*Risk Analysis*)

1. Identifikasi Aset
2. Identifikasi *Thread*
3. Identifikasi Kontrol yang Berlangsung
4. Identifikasi *Vulnerability*
5. Identifikasi *Risk Consequences*
6. Estimasi Risiko (*Risk Estimation*)
   - Evaluasi Risiko (*Risk Evaluation*)
   - Penanganan Risiko (*Risk Threatment*)
   - Penerimaan Risiko (*Risk Acceptance*)

3. Mengukur *Maturity Level*

Mengukur tingkat kematangan (*Maturity Level*) dimulai dengan pengumpulan data dari hasil kuesioner, melakukan perhitungan atau pengujian, melakukan *maturity level* saat ini. Pengukuran tingkat kematangan merujuk pada tingkat kematangan CMMI (*Capability Maturity Model Integration*). Berikut perhitungan matematisnya:

p-ISSN 2088-5407
e-ISSN 2621-9001

$$\overline{X} = \frac{1}{n}\sum_{i=1}^{n} Xi$$

Keterangan :

$\overline{X}$	=	Nilai rata-rata
N	=	Jumlah responden yang mengisi jawaban valid
Xi	=	Nomor urut soal ke-i
$i=1$	=	Urutan soal (soal dimulai dari nomor ke 1)

Gambar 4. Rumus Perhitungan Kuesioner

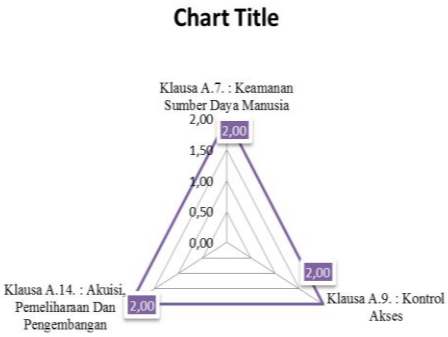
4. Analisis Temuan

Analisis temuan dibuat dari mengukur *Maturity Level* sebelumnya. Analisis temuan tujuannya untuk menentukan strategi penerapan pengembangan kontrol keamanan. Hasil dari analisis temuan tersebut dijadikan acuan untuk perbaikan kontrol keamanan. Berikut hasil Analisis Temuan dari keseluruhan *Maturity Level* Klausa A.7 Keamanan Sumber Daya Manusia, Klausa A.9 Kontrol Akses, Klausa A.14 Akuisis, Pemeliharaan dan Pengembangan :

Tabel 1 Hasil *Maturity Level* Klausa A.7, Klausa A.8, Klausa A.9

Klausa	*Maturity Level*
Klausa A.7. : Keamanan Sumber Daya Manusia	2
Klausa A.9. : Kontrol Akses	2
Klausa A.14. : Akuisi, Pemeliharaan Dan Pengembangan	2
Rata-Rata *Maturity Level*	**2**

Berikut diagram radarnya:



Gambar 5. Radar Nilai Rata-Rata *Maturity Level* Penerapan Kontrol Keamanan yang Sedang Berlangsung

a. Target *Maturity Level*

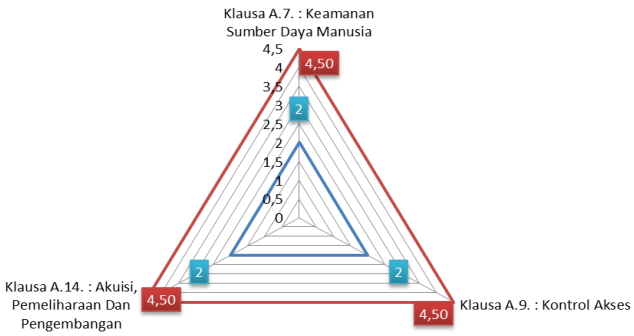
Target *maturity level* dilakukan untuk menemukan kekurangan yang harus dilengkapi oleh organisasi dalam proses penerapan keamanan informasi terhadap seluruh klausa yang sudah ditentukan.

Tabel 2 Nilai Target Pencapaian (GAP)

Klausa (Objektif Kontrol)	*Maturity Level*	Objektif Kontrol	Kontrol Keamanan
	Sedang Berlangsung	Target	GAP
Klausa A.7. : Keamanan Sumbe Daya Manusia	2	4,50	2,50
Klausa A.9. : Kontrol Akses	2	4,50	2,50
Klausa A.14. : Akuisi, Pemeliharaan Dar Pengembangan	2	4,50	2,50
Rata-Rata *Maturity Level*	2,00	4,50	2,50

p-ISSN 2088-5407
e-ISSN 2621-9001

Berikut keterangan gambar radar dari hasil nilai target pencapaian (GAP):



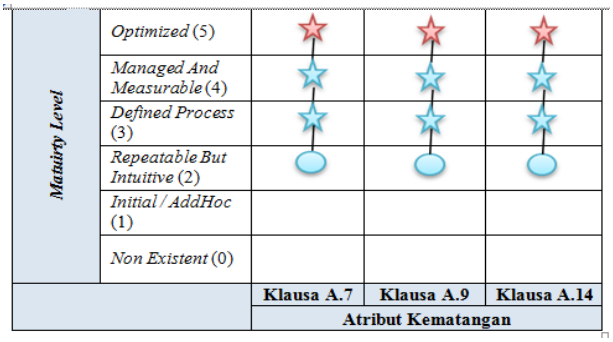
Gambar 6. Diagram Radar GAP Nilai Rata-Rata sedang Berlangsung Dan Target Pencapaian

b. Strategi Pencapaian *Maturity Level*

Dari hasil perhitungan pengukuran *Maturiy Level* yang sedang berlangsung dan yang dicapai memliki nilai GAP *Maturity Level* sangat besar untuk mencapai target yang maksimal. Hasi penerapan analisis manajemen risiko Keamanan Informasi pada kontrol keamanan yang dikelola DISKOMINFO Kota Sukabumi sesuai dengan klausa yang sudah ditentukan yaitu A.7:Keamanan Sumber Daya Manusia, A.9:Kontrol Akses, A.14:Akuisi Pemeliharaan Dan Pengembangan SNI ISO 27001:2013 dan SNI ISO/IEC 31000:2009 *Maturity Level* masih memiliki tingkat yang sangat kecil atau belum sesuai harapan. Strategi pencapaian *maturity level* harus mempertimbangkan tahapan sebagai berikut:

1. Untuk mencapai tahapan nilai *maturity* harus dilalui dengan adanya proses pembelajaran dan perbaikan kepada seluruh pimpinan, administrator, staf/pegawai dan pihak ketiga
2. Minimal sebelum mencapai nilai *maturity* yang *optimized* dilakukannya proses keseimbangan dari seluruh kontrol keamanan yang ditentukan
3. Setelah melakukan evaluasi dilakukan perbaikan dimulai dari *maturity* yang lebih rendah dan selanjutnya dilakukan secara bertahap sampai mendapatkan *level* yang *optimized*.

Berikut gambaran tahapan untuk mencapai nilai *maturity* yang diharapkan dengan melakukan strategi pencapaian *maturity level*, digambarkan sebagai berikut:



Gambar 7. Diagram *Star* Pencapaian *Maturity Level*

5. Perancangan Sistem Manajemen Keamanan Informasi

Perancangan Sistem Manajemen Keamanan Informasi yang akan diterapkan dalam organisasi Pemerintahan di DISKOMINFO Kota Sukabumi berupa dokumen. Dokumen tersebut dibentuk mejadi beberapa bagian, diantaranya Manual Keamanan Informasi (MKI), Prosedur Keamanan Informasi (PKI), Intruksi Kerja (IK), dan Formulir Keamanan Informasi (FKI). Langkah perancangan SMKI dengan

p-ISSN 2088-5407
e-ISSN 2621-9001

melakukan Manajemen Risiko menggunakan SNI ISO/IEC 31000:2009 dan Pengukuran Tingkat Kematangan (*Maturity Level*).

6. Membuat *Statement of Applicability* (SoA)

Statement of Applicability (SoA) adalah dokumen rencana implementasi untuk menentukan pelaksanaan pelatihan (*awarness and training*) SMKI kepada seluruh pegawai. Dimana di dalam dokumen tersebut menjelaskan kontrol keamanan informasi berdasarkan SNI ISO/IEC 27001:2013.

7. Evaluasi Sistem Manajemen Keamanan Informasi

Evaluasi Sistem Manajemen Keamanan Informasi dilakukan untuk menjaga bahwa SMKI selalu sesuai dengan kebutuhan organisasi, selalu ditinjau ulang, dikoreksi dan diperbaiki sesuai dengan kebutuhan organisasi.

8. Saran Dan Perbaikan

Saran dan perbaikan merupakan tahapan terakhir dalam PDCA, tahapan ini termasuk kedalam tahapan *act* yang memberikan penjelasan secara menyeluruh mengenai saran dan perbaikan yang harus dilakukan serta menindaklanjuti perbaikan untuk meningkatkan Keamanan Informasi di dalam organisasi DISKOMINFO lingkungan PEMDA Kota Sukabumi.

KESIMPULAN

Hasil dari penelitian didapatkan suatu penjelasan secara ringkas dalam bentuk kesimpulan. Berikut kesimpulan yang didapat:

1. DISKOMINFO telah diatur dan dilaksanakan keamanan informasi terhadap aset dan informasi tetapi belum didokumentasi dan disosialisasi penerapannya di dalam organisasi.
2. Sesuai hasil penilaian risiko dari 25 profil risiko dalam skenario insiden, didapat penilaian 1 risiko dengan tingkat sangat tinggi (*critical*), 1 risiko dengan tingkat tinggi (*high*), 6 risiko dengan tingkat medium (*moderate*) dan yang terakhir 17 risiko dengan tingkat rendah (*low*).
3. Sedangkan hasil *maturity level* pada penerapan kontrol keamanan untuk klausa A.7, klausa A.9 dan klausa A.14, didapatkan hasil temuan sebagai berikut:

Tabel 3 Hasil Rata-Rata *Maturity Level*

Klausa	*Maturity Level*	Definisi
Klausa A.7. : Keamanan Sumber Daya Manusia	2,00	*Repeatable*
Klausa A.9. : Kontrol Akses	2,00	*Repeatable*
Klausa A.14. : Akuisi, Pemeliharaan Dan Pengembangan	2,00	*Repeatable*
Rata-Rata *Maturity Level*	2,00	

4. Hasil dari Analisis Sistem Manajemen Keamanan Informasi menggunakan SNI ISO/IEC 27001:2013 dan SNI ISO/IEC 31000:2009 adalah dapat diketahui ruang lingkup SMKI di DISKOMINFO, *risk*

management untuk mengetahui profil risiko, operasional atau pelaksanaan SMKI, tinjauan SMKI dan saran perbaikan atau pengendalian gangguan terhadap infrastruktur TI yang memiliki masalah keamanan informasi sehingga terjadinya peretasan di DISKOMINFO Kota Sukabumi. Selanjutnya dibuatkan dokumen Manual Keamanan Informasi, Prosedur Keamanan Informasi, Intruksi Kerja dan Formulir Keamanan Informasi.

UCAPAN TERIMA KASIH

Penulis ucapkan Puji Syukur kepada Allah SWT yang telah memudahkan setiap langkah untuk menyelesaikan tesis dan memberikan energi ruhiyah yang positif. Terima kasih kepada Pak Ashwin dan Pak Hendayun atas waktu dan ilmu yang diberikan sehingga membantu Penulis dalam penyusunan tesis ini. Selanjutnya terima kasih kepada Suami dan Orang Tua yang telah memberikan Doa, dukungan dan motivasi untuk menyelesaikan tesis ini.

DAFTAR PUSTAKA

[1] TechnoID. Situs Resmi Pemda Kota Diserang Hacker : Sukabumi. Tersedia Online Di : https://www.techno.id/social/situs-resmi-pemkot-sukabumi-sedang-diserang-hacker-1504109.html.

[2] InfoKomputer. Hacker : Halaman 4. Tersedia Online Di : https://infokomputer.grid.id/tag/hacker/page/4/

[3] NasionalKompas. Siber Nasional : Indonesia. Tersedia Online Di : http://nasional.kompas.com/read/2017/01/11/06591651/apa.urgensinya.badan.siber.nasional.untuk.indonesia.

[4] Menteri Komunikasi Dan Informatika. 2016. Perlindungan Data Pribadi Dalam Sistem Elektronik Nomor 20 Tahun 2016. Republik Indonesia.

[5] Riadi, Imam & Rosmiati. 2016. Analisis Keamanan Informasi Berdasarkan Kebutuhan Teknikal Dan Operasional Mengkombinasikan Standar *ISO 27001:2005* dengan *Maturity Level.* Seminar Nasional Teknologi Informasi dan Multimedia: Yogyakarta.

[6] ReferensiElsam. UU Nomor 23 Tahun 2014. Pemerintahan Daerah. Tersedia Online Di : http://referensi.elsam.or.id/2015/01/uu-nomor-23-tahun-2014-tentang-pemerintah-daerah/

[7] Unhas. Form Peraturan. UU Nomor 19 Tahun 2016 Perubahan ITE Dari UU No 11 Tahun 2008. Tersedia Online Di :http://htl.unhas.ac.id/form_peraturan/photo/103211-UU-Nomor-19-Tahun-2016%20tentang%20informasi%20dan%20Transasksi%20Elektronik.pdf

[8] Kominfo. Produk Hukum. Peraturan Pemerintah Republik Indonesia No 82 Tahun 2012. Tersedia Online Di :

https://jdih.kominfo.go.id/produk_hukum/view/id/6/t/peraturan+pemerintah+republik+indonesia+nomor+82+tahun+2012

[9] Kominfo. Produk Hukum. Peraturan Menteri Komunikasi Dan Informatika No 4 Tahun 2016. Tersedia Online Di : https://jdih.kominfo.go.id/produk_hukum/view/id/532/t/peraturan+menteri+komunikasi+dan+informatika+nomor+4+tahun+2016+tanggal+11+april+2016.

[10] Candiwan. Priyadi, Yuze Yudi, & Yuni Cintia. 2016. Analisis Sistem Manajemen Keamanan Informasi Menggunakan *ISO/IEC 27001:2013* Serta Rekomendasi Model Sistem Menggunakan *Data Flow Diagram* Pada Direktorat Sistem Informasi Perguruan Tinggi. Jurnal Sistem Informasi. Universitas Telkom.

[11] Silanegara, Indra & Bayu Adhi Tama. 2015. Strategi Pemilhan Kontraktor Perangkat Lunak Dengan Memanfaatkan Pengetahuan Terhadap *Capability Maturity Model Integration for development (CMMI for Dev)*. Universitas Sriwijaya. Jakarta.

[12] Sugiyono. 2013. Metode Penelitian Pendekatan Kuantitatif, Kualitatif dan R&D. Alfa Beta: Bandung.

[13] Ariansyah, Edwin. 2016. Perancangan Sistem Informasi *Tracking* Pengiriman Barang Berbasis *Web* Pada PT Satu Nusantara Abadi Jakarta Timur. Tugas Akhir. STMIK Raharja.

[14] Sobri, Muhammad, Emigawaty, & Nita Rosa Damayanti. 2017. Pengantar Teknologi Informasi. Andi. Yogyakarta.

[15] Hutahean, Jeperson. 2015. Konsep Sistem Informasi. CV Budi Utama. Yogyakarta.

[16] Yuhefizar, Ir. HA Mooduto, & Rahmat Hidayat. 2009. Cara Mudah Membangun *Website Interaktif Menggunakan Context Management System Joomla*. Edisi Revisi. PT Elex Media Komputindo. Jakarta.

[17] Ayuningtyas, Nuriana. 2009. Implementasi Ontologi *Web* Aplikasi Semantik Untuk Sistem Sitasi Jurnal Elektronik Indonesia. Tugas Akhir.

[18] Sibero, Alexander F K. 2014. *Web Programming Power Pack*. MediaKom. Yogyakarta.

[19] Checkmarx. 2016. *The Important Of Database Security And Integrity*. Tersedia Online Di : https://www.checkmarx.com/2016/06/24/20160624the-importance-of-database-security-and-integrity/

[20] Badan Standarisasi Nasional. 2016. Penetapan Standarisasi Nasional Indonesia SNI ISO/IEC 27001:2013 Nomor 61/KEP/BSN/4/2016. Sistem Manajemen Keamanan Informasi.

[21] Sarno, Riyanarto & Irsyat Iffano. 2009. *Sistem Manajemen Keamanan Informasi Berbasis ISO 27001*. ITSPRESS: Bandung.

[22] Christina, D. 2012. Asesmen Risiko Berbasis SNI ISO/IEC 31000:2009. Diunduh dari: http://dianechristina.wordpress.com/2012/10/22/asesmen-manajemen-risiko-berbasis-iso-310002009/

[23] Cahyono Hadi M & Andi Rafiandi. 2010. Jurus Sukses Sertifikasi ISO 27001. Andita Publishing. Jakarta

[24] Tjiptardjo Mochamad. 2010. Kebijakan Tata Kelola Teknologi Informasi Dan Komunikasi Direktorat Jenderal Pajak Nomor : PER-37/PJ/2010.

[25] Sekretariat Daerah Kota Sukabumi. 2012. Berita Daerah Kota Sukabumi : Peraturan Walikota Sukabumi (Kedudukan, Tugas Pokok, Fungsi, Dan Tata Kerja Kantor Komunikasi Dan Informatika Kota Sukabumi) No 50. Bagian Hukum. Sukabumi.

[26] Sekretariat Daerah Kota Sukabumi. 2016. Berita Daerah Kota Sukabumi Nomor 9 dan Nomor 44: Kedudukan, Susunan Organisasi, tugas Pokok, Fungsi, dan Tata Kerja Dinas Komunikasi dan Informatika Kota Sukabumi. Bagian Hukum. Sukabumi.

[27] Tim Direktorat Keamanan Informasi. 2011. Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik. Edisi 2.0. Kominfo