Perencanaan Tata Kelola Keamanan Informasi dalam Penerapan Cloud Computing Menggunakan ISO 27001:2013 pada PT.SPINDO,Tbk

Diana Anggraini[1], Rahadian Bisma[2]

[1,2] Jurusan Teknik Informatika/Sistem Informasi, Universitas Negeri Surabaya
[1]dianaanggraini16051214028@mhs.unesa.ac.id
[2]rahadianbisma@unesa.ac.id

Abstrak*— PT.SPINDO,Tbk merupakan sebuah perusahaan dengan kapasitas produksi terbesar di Indonesia sebagai penghasil pipa baja. Sebagai perusahaan dengan aktivitas produksi besar, PT.SPINDO,Tbk ingin menerapkan layanan *mail server* berbasis *cloud computing* untuk memudahkan komunikasi namun tetap secara professional. Layanan *cloud computing* menjadi layanan yang paling diminati oleh perusahaan karena memberikan kemudahan dan kenyamanan diakses dimana saja melalui jaringan internet serta dapat menghemat biaya infrastruktur TIK. Namun, disamping kemudahan dan kenyamanan yang disediakan layanan *cloud computing* terdapat berbagai macam ancaman antara lain *multi-tenant*, kehilangan data, kehilangan kontrol, proteksi data dan privasi, serta penurunan performa. Ancaman dalam penerapan *cloud computing* sebagian besar terkait pada lingkup keamanan informasi. Permasalahan tersebut dapat diatasi dengan perencanaan tata kelola keamanan informasi yang baik. Perencanaan tata kelola keamanan informasi pada penelitian ini menggunakan SNI ISO 27001:2013 sebagai acuan kontrol keamanan informasi. Penelitian ini menggunakan metode OCTAVE dengan pendekatan evaluasi risiko terhadap aspek CIA. Hasil penelitian berupa perencanaan kebijakan dan prosedur yang diperlukan untuk menjaga keamanan informasi dalam penerapan layanan berbasis *cloud computing.

***Kata Kunci*— tata kelola keamanan informasi, ISO 27001:2013, analisa risiko, metode octave.**

I. PENDAHULUAN

Penggunaan *cloud* computing pada saat ini merupakan sebuah evolusi dari teknologi informasi yang memberikan kemudahan dan kenyamanan dalam menyediakan layanan maupun produk sesuai permintaan pengguna yang dapat diakses dimana saja melalui jaringan internet. Sehingga, penggunaan *cloud computing* menjadi layanan yang paling diminati oleh perusahaan. PT.SPINDO,Tbk merupakan merupakan sebuah perusahaan dengan kapasitas produksi terbesar di Indonesia sebagai penghasil pipa baja [1]. Sebagai perusahaan dengan aktivitas produksi besar, PT.SPINDO,Tbk ingin menerapkan layanan *mail server* berbasis *cloud computing* untuk memudahkan komunikasi namun tetap secara professional. Mail server sendiri merupakan layanan internet atau *server* berbasis *cloud* computing yang berfungsi seperti email [2]. Kelayakan pertukaran informasi melalui layanan *mail server* berbasis *cloud computing* perlu diatasi terlebih dahulu sebelum dilakukan penerapan dikarenakan dalam penerapan layanan berbasis *cloud computing* terdapat berbagai ancaman yaitu *multi-tenant*, kehilangan data, kehilangan kontrol, proteksi data dan privasi, serta penurunan performa [3].

Ancaman dalam penerapan *cloud computing* sebagian besar terkait pada lingkup keamanan informasi. Karena adanya ancaman tersebut menimbulkan keraguan terhadap penerapan *cloud computing* pada perusahaan berskala besar seperti PT.SPINDO,Tbk. Berdasarkan permasalahan keraguan penerapan layanan *cloud computing* karena berbagai ancaman keamanan informasi yang dapat terjadi dibutuhkan perencanaan tata kelola keamanan informasi yang baik. Perencanaan tata kelola keamanan informasi yang baik menjadi aspek yang perlu diperhatikan dalam penerapan *cloud computing* karena informasi termasuk aset yang sangat penting bagi keberlangsungan perusahaan. Tata kelola keamanan informasi didefinisikan sebagai suatu sistem yang mengatur dan mengarahkan segala aktivitas terkait keamanan informasi di sebuah organisasi [4].

Penggunaan *framework* tata kelola keamanan informasi dapat dijadikan pilihan untuk menciptakan kombinasi yang sesuai dalam menjaga keamanan informasi. *Framework* yang dapat digunakan sebagai pedoman dalam perancangan tata kelola keamanan informasi terdapat beragam jenis diantaranya ISO 27001, COSO, COBIT, dan lain sebagainya. Masing-masing *framework* tersebut memiliki fungsi, kelemahan dan kelebihan masing-masing, berikut perinciannya [5];

TABEL I PERBEDAAN STANDAR KEAMANAN INFORMASI

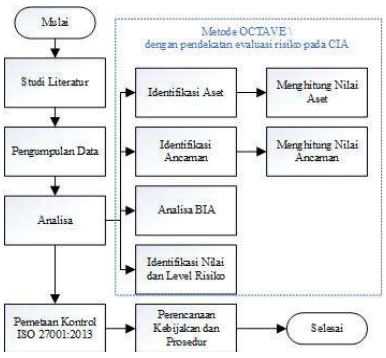
	ISO 27001:2013	COBIT 5	COSO
Fungsi	Membangun dan memelihara sistem manajemen keamanan informasi guna melindungi aset informasi yang dapat diterapkan secara fleksibel	Menyediakan sebuah *framework* yang berfokus terhadap praktik dalam manajemen teknologi informasi	Kerangka pengendalian yang bersifat internal untuk memberikan jaminan mengenai pencapaian tujuani dalam efektivitas dan efisiensi operasi
Lingkup Area	10 klausul 14 kontrol area 35 kontrol objektif 114 kontrol keamanan informasi	5 domain 37 proses	5 komponen 20 proses
Kelebihan	Dapat diterapkan	Dapat	Membantu

	diberbagai jenis organisasi, membantu dalam pembangunan dan peningkatan SMKI	meningkatkan efektivas biaya karena integrasi yang memudahkan	mencapai kinerja dan profitabilitas dari target
Kelemahan	Memerlukan serangkaian seri lain agar lebih mendetail	Hanya berpusat terhadap titik kontrol yang ditentukan	Tidak dapat menjamin kelangsungan kontrol internal

Berdasarkan tabel tersebut ISO 27001 lebih unggul dalam fleksibilitas penerapan yang dapat dikembangkan sesuai dengan kebutuhan organisasi, tujuan organisasi dan persyaratan keamanan. ISO 27001:2013 merupakan sebuah standar yang bersifat independent terhadap produk teknologi informasi, pendekatan yang digunakan yakni manajemen risiko, dan dibuat dapat menjamin dan memberi keyakinan terhadap perusahaan yang memilih kontrol keamananan untuk melindungi aset informasi [6]. Standar tersebut sangat populer digunakan untuk meminimalisir risiko dan ancaman terkait keamanan informasi. Dalam ISO 27001:2013 terdapat panduan yang dapat diaplikasikan dalam penerapan keamanan informasi untuk mencapai sasaran keamanan informasi yang akan dikendalikan dengan tepat. ISO 27001:2013 memiliki 14 klausul, 35 kontrol objektif dan 114 kontrol keamanan yang dapat dipilih untuk diimplementasikan dalam SMKI [7].

Maka dari itu, dalam penelitian ini perencanaan tata kelola keamanan informasi pada *cloud* dibuat berdasarkan SNI ISO/IEC 27001:2013 dengan tambahan refrensi dari ISO/IEC 27017:2015 dimana standar ini merupakan standar pengendalian keamanan informasi untuk *cloud computing* yang dapat membantu menanggulangi risiko dan ancaman keamanan informasi pada layanan *cloud computing.* Penilitian dilakukan dengan menggunakan metode OCTAVE melalui pendekatan evaluasi risiko dari 3 aspek keamanan informasi yakni *confidentially, integrity* dan *avaibility (CIA).* Hasil dari penelitian ini berupa rincian dokumen perencanaan tata kelola keamanan informasi yang perlu dibuat berdasarkan evaluasi risiko yang dilakukan dengan kontrol objektif dan keamanan pada ISO 27001:2013.

II. METODE



Gambar 1 Tahapan Penelitian

Berikut penjelasan mengenai tahapan-tahapan dalam penelitian berdasarkan gambar 1

A. *Studi Literatur*

Dalam tahap studi literatur dilakukan proses mengumpulkan dan mempelajari teori yang berhubungan dengan topik penelitian yang didapat baik dari buku, jurnal ilmiah, materi mengenai perusahaan yang akan diteliti dan skripsi yang digunakan sebagai dasar dari penelitian ini. Referensi jurnal dan skripsi terdahulu yang digunakan dalam penelitian ini membahas tentang isu keamanan informasi pada cloud computing, perancangan tata kelola keamanan informasi, serta penerapan tata kelola keamanan informasi menggunakan standar ISO/IEC 27001. Berdasarkan studi literatur yang telah dilakukan dipilih ISO 27001:2013 sebagai standar untuk merencanakan tata kelola keamanan informasi dan penngunaan metode OCTAVE dalam evaluasi risiko terhadap aspek keamanan informasi CIA.

B. *Pengumpulan Data*

Pengumpulan data didefinisikan sebagai suatu aktivitas yang dilakukan untuk mendapatkan informasi yang diperlukan dalam mencapaih tujuan dari suatu penelitian [8]. Metode yang digunakan dalam penelitian ini adalah wawancara. Wawancara dilakukan kepada pihak dari perusahaan yang bersangkutan dengan penelitian ini.

C. *Analisa*

Metode analisa yang diaplikasikan dalam penelitian yang dilakukan penulis adalah metode OCTAVE menggunakan pendekatan evaluasi risiko terhadap aspek keamanan informasi CIA. Metode OCTAVE *(The Operationally Critical Threat, Asset, and Vulnerability Evaluation)* merupakan sebuah pendekatan yang bertujuan untuk mengatur dan mengendalikan risiko pada keamanan informasi yang dikembangkan oleh *Software Engineering Institute, Carnegie Mellon University*, 1999 [9].

Berikut tahapan yang dilakukan dalam penelitian ini berdasarkan metode yang digunakan:

1) *Identifikasi Aset:* Tahap yang dilakukan paling awal dari proses ini yaitu mengidentifikasi aset milik perusahaan yang mendukung penerapan layanan mail server berbasis cloud. Kemudian dihitung nilai dari masing-masing aset berdasarkan pendekatan CIA. Hasil dari tahap ini adalah nilai aset (NA) yang digunakan untuk mencari nilai risiko (NR).

2) *Identifikasi Ancaman:* Mengidentifikasi ancaman dan kelemahan pada masing-masing aset yang dapat mengganggu berlangsungnya proses bisnis, setelah itu menetapkan nilai ancaman pada masing-masing aset. Hasil dari tahap ini adalah nilai ancaman (NT) yang digunakan untuk mencari nilai risiko (NR).

3) *Analisis BIA (Business Impact Analysis):* Menganalisa dampak bisnis (Business Impact Analysis) PT.SPINDO,Tbk dalam menerapkan cloud computing. Proses ini dilakukan untuk mendapatkan Nilai BIA

(Business Impact Analysis) yang digunakan untuk mengetahui nilai risiko (NR).

4) *Identifikasi Nilai dan Level Risiko:* Proses ini bertujuan untuk mengetahui nilai risiko dan menentukan level risiko yang terjadi berdasarkan kriteria dampak dan probabilitas ancaman dengan membuat tabel matriks.

D. *Pemetaan Kontrol ISO 27001:2013*

Dalam tahap ini dilakukan pemilihan kontrol keamanan informasi pada *cloud* yang disesuaikan dengan penilaian risiko yang telah dilakukan dan ISO 27001:2013 sebagai landasan.

E. *Perencanaan Kebijakan dan Prosedur*

Dalam tahap ini dilakukan perencanaan SOP *(Standart Operational Procedur*e) yang diperlukan dalam penerapan *cloud computing* berdasarkan ISO 27001:2013 dan ISO 27017:2015 sebagai referensi tambahan

III. HASIL DAN PEMBAHASAN

Berdasarkan hasil studi literatur dan pengumpulan data yang telah dilakukan. Informasi yang diperoleh untuk kebutuhan penelitian dikelola melalui tahapan-tahapan berikut:

A. *Identifikasi Aset*

Tahap ini dilakukan untuk mengetahui aset-aset penting yang mendukung proses bisnis dalam layanan mail server yang akan diterapkan. Berdasarkan hasil wawancara berikut daftar aset-aset terkait:

TABEL II IDENTIFIKASI ASET

No	Kategori Aset	Daftar Aset
1.	Hardware	Server
		PC Client
2.	Network	Router
		Switch
		Modem
		Access Point
		Kabel
3.	Software	Linux
4.	Information	Data Kepegawaian
		Jadwal Rapat
		Laporan Keuangan
		Data Kegiatan Produksi
		Data Proyek
		Data Aset
		Data User dan Password
5.	Human Resources	Pegawai

B. *Menghitung Nilai Aset*

Proses menghitung nilai aset didasari dengan beberapa aspek pendukung yakni kerahasiaan (confidentiality), keutuhan (integrity) dan ketersediaan (avaibility) dengan rumus[10]:

NA = NC+NI+NV.

Berikut tabel hasil perhitungan nilai aset yang nantinya akan digunakan dalam perhitungan Nilai Risiko:

TABEL III NILAI ASET

No.	Daftar Aset	Kriteria			Nilai Aset
		NC	NI	NV	
1.	Server	4	4	4	12
2.	PC Client	2	1	2	5
3.	Router	3	2	4	9
4.	Switch	3	2	4	9
5.	Access point	3	2	4	9
6.	Modem	3	1	4	8
7.	Kabel LAN	3	2	3	8
8.	Linux	3	3	3	9
9.	Data Kepegawaian	4	4	3	11
10.	Jadwal Rapat	2	2	2	6
11.	Laporan Keuangan	4	4	4	12
12.	Data Kegiatan Produksi	3	4	3	10
13.	Data Proyek	3	4	3	10
14.	Data Aset	3	2	3	8
15.	Data User dan Password	4	3	3	10
16.	Pegawai	3	3	3	9

C. *Identifikasi Ancaman dan Kelemahan*

Proses ini dilakukan untuk mengetahui ancaman dan kelemahan yang terdapat dan dapat membahayakan sistem maupun proses bisnis. Berikut hasil identifikasi ancaman dan kelemahan pada aset

TABEL IV IDENTIFIKASI ANCAMAN DAN KELEMAHAN

No.	Kategori Aset	Daftar Aset	Ancaman dan Kelemahan
1.	Hardware	Server	• Bencana alam • Kerusakan server • Server down • Kesalahan dalam konfigurasi dan perawatan • Kapasitas penyimpanan penuh • Terserang malware atau virus • Pencurian komponen server • Adanya akses illegal • Kehilangan data • Hilangnya voltase listrik
		PC Client	• Bencana alam • Kerusakan • Kesalahan dalam konfigurasi dan perawatan • Terserang virus • Pencurian komponen • Adanya Akses ilegal • Kehilangan data • Hilangnya voltase listrik

2.	Network	Router Switch Access Point Modem Kabel LAN	• Kerusakan hardware • Kabel terputus • Hilangnya komponen • Terserang virus • Adanya akses illegal • Penyadapan informasi melalui jaringan • Pembobolan jaringan • Kesalahan dalam pengalamatan IP • Kesalahan konfigurasi • Kualitas jaringan buruk • Monopoly bandwich • Hilangnya voltase listrik • Gangguan kabel
3.	Software	Linux	• Terserang malware atau virus • Kesalahan pada program (bugs) • Kesalahan saat memasukkan data • Eksekusi program yang salah • Penyadapan oleh orang dalam • Adanya akses illegal
4.	Information	Data Kepegawaian Jadwal Rapat Laporan Keuangan Data Kegiatan Produksi Data Proyek Data Aset Data User Dan Password	• Data hilang • Data corrupt • Data tidak memiliki backup • Kesalahan saat memasukkan data • Pemalsuan informasi saat membuat laporan • Pencurian data • Penggunaan user dan password oleh orang lain • Penggunaan password tidak diubah-ubah
5.	Human Resources	Pegawai	• Penyalahgunaan hak akses dan wewenang • Tidak memperhatikan prosedur yang berlaku • Penyalahgunaan data organisasi • Password shared • Pemalsuan data • Kesalahan dalam input/delete data

D. *Identifikasi Nilai Ancaman*

Nilai ancaman didapatkan dari perhitungan rata-rata dari jumlah probabilitas dengan jumlah ancaman yang teridentifikasi. yang dapat dituliskan dengan rumus [10]:

NT = ∑ Probabilitas / ∑ Ancaman

Hasil dari proses identifikasi nilai ancaman pada masing-masing aset dapat dilihat pada tabel rekap berikut ini yang nantinya akan digunakan dalam perhitungan Nilai Risiko:

TABEL V NILAI ANCAMAN

No	Daftar Aset	Nilai Ancaman
1.	Server	0,41
2.	PC Client	0,49
3.	Router	0,51
4.	Switch	0,51
5.	Access point	0,51
6.	Modem	0,54
7.	Kabel LAN	0,53
8.	Linux	0,40
9.	Data Kepegawaian	0,44
10.	Jadwal Rapat	0,47
11.	Laporan Keuangan	0,46
12.	Data Kegiatan Produksi	0,47
13.	Data Proyek	0,47
14.	Data Aset	0,50
15.	Data User dan Password	0,48
16.	Pegawai	0,42

E. *Analisa Dampak Bisnis*

Dalam proses Analisa Dampak Bisnis dilakukan untuk mengetahui Nilai BIA pada masing-masing aset yang telah diidentifikasi melalui pendekatan aspek keamanan informasi CIA sebelumnya. Nilai BIA pada masing-masing aset dapat dilihat pada tabel di bawah ini yang nantinya akan digunakan dalam perhitungan Nilai Risiko:

TABEL VI ANALISA DAMPAK BISNIS

No	Daftar Aset	Dampak	Nilai BIA	Skala BIA
1.	Server	Proses bisnis yang berkaitan dengan server terganggu	4	*Very High Critical*
2.	PC Client	Pekerjaan terganggu	3	*High Critical*
3.	Router	Jaringan internet tidak tersedia serta tidak dapat melakukan pengiriman data	3	*High Critical*
4.	Switch	Jaringan internet tidak tersedia serta tidak dapat melakukan pengiriman data	3	*High Critical*
5.	Access Point	Jaringan internet tidak tersedia serta tidak dapat melakukan pengiriman data	3	*High Critical*
6.	Modem	Jaringan internet tidak tersedia	3	*High Critical*
7.	Kabel LAN	Jaringan internet tidak tersedia serta tidak dapat melakukan pengiriman data	1	*Low Critical*
8.	Linux	Aplikasi crash sehingga pekerjaan Terganggu	2	*Mayor Critical*
9.	Data Kepegawaian	Pelaporan monitoring data kepegawaian Terganggu	2	*Mayor Critical*
10.	Jadwal Rapat	Waktu pelaksanaan rapat tertunda	3	*High Critical*

11.	Laporan Keuangan	Pelaporan monitoring data keuangan tertunda	4	*Very High Critical*
12.	Data Kegiatan Produksi	Pelaporan monitoring data kegiatan produksi terganggu	4	*Very High Critical*
13.	Data Proyek	Pelaporan monitoring data proyek terganggu	4	*Very High Critical*
14.	Data Aset	Pelaporan monitoring aset tertunda	2	*Mayor Critical*
15.	Data User dan Password	Pengguna tidak memiliki kontrol akses sehingga terdjadi akses ilegal	4	*Very High Critical*
16.	Pegawai	Penyalahgunaan hak akses dan akses ilegal terhadap informasi penting	2	*Mayor Critical*

F. *Identifikasi Nilai dan Level Risiko*

Dalam proses ini dilakukan identifikasi untuk mengetahui tingkat risiko jika dikaitkan dengan dampak dan probabilitas ancaman pada masing-masing aset. Identifikasi risiko dilakukan dengan menempatkan masing-masing dampak dan probabilitas pada aset ke dalam matriks yang telah ditentukan berikut ini [10]:

TABEL VI MATRIKS LEVEL RISIKO

Probabilitas ancaman	**Dampak**				
	Not Critical (20)	Low Critical (40)	Mayor Critical (60)	High Critical (80)	Very High Critical (100)
Low (0,1)	Low 2	Low 4	Low 6	Low 8	Low 10
Medium (0,5)	Low 10	Medium 20	Medium 30	Medium 40	Medium 50
High (1,0)	Low 20	Medium 40	Medium 60	High 80	High 100

Untuk dapat mengetahui letak level resiko pada matriks maka diperlukan perhitungan nilai resiko menurut metode OCTAVE dengan rumus [10]:

NR = NAxBIAxNT.

Berikut hasil perhitungan nilai resiko yang dilakukan pada masing-masing aset:

TABEL VII IDENTIFIKASI NILAI DAN LEVEL RISIKO

Kategori Aset	**Daftar Aset**	**NA**	**BIA**	**NT**	**Nilai Risiko**	**Level Resiko**
Hardware	Server	12	4	0,41	19,68	*Medium*
	PC	5	3	0,49	7,35	*Low*
Network	Router	9	3	0,51	13,77	*Medium*
	Switch	9	3	0,51	13,77	*Medium*
	Access Point	9	3	0,51	13,77	*Medium*
	Modem	8	3	0,54	12,96	*Medium*
	Kabel LAN	8	1	0,53	4,24	*Low*
Software	Linux	9	2	0,40	7,2	*Low*
Information	Data Kepegawaian	11	2	0,44	9,68	*Low*
	Jadwal Rapat	6	3	0,47	8,46	*Low*
	Laporan Keuangan	12	4	0,46	22,08	*Medium*
	Data Kegiatan Produksi	10	4	0,47	18,8	*Medium*
	Data Proyek	10	4	0,47	18,8	*Medium*
	Data Aset	8	2	0,50	8	*Low*
	Data User dan Password	10	4	0,48	19,2	*Medium*
Human Resources	Pegawai	9	2	0,42	7,56	*Low*

Setelah nilai risiko diketahui maka penentuan risiko diterima dapat dilakukan dengan menempatkan nilai risiko pada matriks untuk mengetahui level risiko dan menyesuaikan dengan kriteria penanganan resiko sebagai berikut:

TABEL VIII KRITERIA PENANGANAN RISIKO

Level Risiko	**Tindakan**
Low	Menerima risiko dengan menetapkan kontrol keamanan yang sesuai
Medium	Mengelola risiko dengan memberikan penanganan risiko pada setiap aset yang bernilai medium dengan pengendalian berdasarkan kontrol objektif dan kontrol keamanan yang sesuai dengan ISO 2700M1:2013
High	Menolak risiko, memerlukan rencana tindakan untuk perbaikan

G. *Pemetaan Kontrol Objektif dan Kontrol Keamanan ISO 27001:2013*

Pemilihan kontrol objektif dan keamanan dilakukan berdasarkan hasil identifikasi ancaman masing-masing aset pada tabel 5 pada kontrol objektif dan kontrol keamanan ISO 27001:2013. Berikut referensi kontrol keamanan ISO 27001:2013 yang dipilih pada masing-masing aset [11]:

TABEL IX PEMETAAN REFERENSI KONTROL KEAMANAN ISO 27001:2013

Kategori Aset	**Daftar Aset**	**Level Resiko**	**Referensi Kontrol/Annex A**
Hardware	Server	Medium	A.9.1.1 Kebijakan kontrol akses A.11.2.4 Kontrol pemeliharaan peralatan A.12.2.1 Kontrol terhadap malware A.12.3.1 *Backup* informasi
	PC	Low	
Network	Router	Medium	A.9.1.1 Kebijakan kontrol akses A.9.1.2 Akses ke jaringan dan layanan jaringan A.11.2.3 Keamanan kabel A.11.2.4 Kontrol pemeliharaan peralatan A.13.1.1 Kontrol jaringan A.13.1.2 Keamanan
	Switch	Medium	
	Access Point	Medium	
	Modem	Medium	
	Kabel LAN	Low	

			layanan jaringan
Software	Linux	Low	A.9.1.1 Kebijakan kontrol akses A.9.4.1 Kebijakan pembatasan akses informasi
Information	Data Kepegawaian	Low	A.5.1.1 Kebijakan untuk keamanan informasi A.9.1.1 Kebijakan kontrol akses A.9.2.3 Manajemen hak akses khusus A.9.4.1 Pembatasan hak akses informasi A.9.4.2 Prosedur *log on* yang aman A.9.4.3 Sistem manajemen kata sandi A.12.3.1 *Backup* informasi A.13.2.1 Kebijakan dan prosedur pengalihan informasi A.13.2.3 Pesan elektronik
	Jadwal Rapat	Low	
	Laporan Keuangan	Medium	
	Data Kegiatan Produksi	Medium	
	Data Proyek	Medium	
	Data Aset	Low	
	Data User dan Password	Medium	
Human Resources	Pegawai	Low	A.6.1.1 Peran dan tanggung jawab keamanan informasi A.7.2.2 Kesadaran, Pendidikan dan pelatihan keamanan informasi A.9.1.1 Kebijakan kontrol akses A.9.4.1 Pembatasan hak akses informasi A.9.4.3 Sistem manajemen kata sandi A.12.4.1 Pencatatan kejadian A.12.4.2 Perlindungan informasi *log*

H. *Perencanaan Kebijakan dan Prosedur*

Berdasarkan hasil pemetaan yang telah dilakukan sebelumnya. Didefinisikan beberapa usulan kebijakan dan prosedur terhadap masing-masing kontrol keamanan ISO 27001:2013 yang dijabarkan sebagai berikut:

TABEL X PERENCANAAN KEBIJAKAN DAN PROSEDUR

Kontrol Keamanan	Kebijakan	Prosedur
A.5.1.1 Kebijakan untuk keamanan informasi	Kebijakan Keamanan Informasi	Tidak ada usul prosedur
A.6.1.1 Peran dan tanggung jawab keamanan informasi	Kebijakan Keamanan Informasi	Tidak ada usul prosedur
A.7.2.2 Kesadaran, Pendidikan dan pelatihan keamanan informasi	Kebijakan Pengembangan SDM	SOP Pelatihan dan Pengembangan
A.9.1.1 Kebijakan kontrol akses	Kebijakan Pengendalian Hak Akses	SOP Pengelolaan Hak Akses
A.9.1.2 Akses ke jaringan dan layanan jaringan	Kebijakan Keamanan Jaringan	SOP Pengelolaan Jaringan
A.9.2.3 Manajemen hak akses khusus	Kebijakan Pengendalian Hak Akses	SOP Pengelolaan Hak Akses
A.9.4.1 Pembatasan hak akses informasi	Kebijakan Pengendalian Hak Akses	SOP Pengelolaan Hak Akses
A.9.4.2 Prosedur *log on* yang aman	Kebijakan Keamanan Informasi	SOP Klasifikasi Informasi
A.9.4.3 Sistem manajemen *password*	Kebijakan Keamanan Informasi	SOP Pengelolaan P*assword*
A.11.2.3 Keamanan kabel	Kebijakan Pengelolaan Peralatan	SOP Keamanan Kabel
A.11.2.4 Kontrol pemeliharaan peralatan	Kebijakan Pengelolaan Peralatan	SOP Perawatan Peralatan
A.12.2.1 Kontrol terhadap malware	Kebijakan Keamanan Informasi	SOP Pengelolaan M*alware*
A.12.3.1 *Backup* informasi	Kebijakan Keamanan Informasi	SOP B*ackup* dan *Restore*
A.12.4.1 Pencatatan kejadian	Kebijakan Keamanan Informasi	SOP Klasifikasi Informasi
A.12.4.2 Perlindungan informasi *log*	Kebijakan Keamanan Informasi	SOP Klasifikasi Informasi
A.13.1.1 Kontrol jaringan	Kebijakan Keamanan Jaringan	SOP Pengelolaan Jaringan
A.13.1.2 Keamanan layanan jaringan	Kebijakan Keamanan Jaringan	SOP Pengelolaan Jaringan
A.13.2.1 Kebijakan dan prosedur pengalihan informasi	Kebijakan Keamanan Informasi	SOP Pertukaran Informasi
A.13.2.3 Pesan elektronik	Kebijakan Keamanan Informasi	SOP Pertukaran Informasi

I. *Penjelasan Perencanaan Kebijakan dan Prosedur*

Berdasarkan hasil pemetaan usulan kebijakan dan prosedur terhadap kontrol keamanan ISO 27001:2013 yang telah dilakukan pada tabel 14. Penjelasan dari usulan masing-masing kebijakan dan prosedur didefinisakan sebagai berikut:

TABEL XI PENJELASAN KEBIJAKAN DAN PROSEDUR

No Dokumen	Nama Dokumen	Penjelasan
KB-ICT-01	Kebijakan Keamanan Informasi	Pedoman yang digunakan untuk mencegah terjadinya risiko keamanan informasi Kebijakan ini dibuat berdasarkan standar ISO 27001:2013 pada klausul A.5.1.1, A.6.1.1, A.9.4.2, A.9.4.3, A.12.2.1, A.12.3.1, A.12.4.1, A.12.4.2, A.13.2.1, dan A.13.2.3.
KB-ICT-02	Kebijakan Pengendalian Hak Akses	Pedoman mengenai pengelolaan hak akses yang bertujuan untuk mencegah terjadinya risiko terkait keamanan informasi. Kebijakan ini dibuat berdasarkan standar ISO 27001:2013 pada klausul A.9.1.1, A.9.2.3, dan A.9.4.1.
KB-ICT-03	Kebijakan Pengembangan SDM	Pedoman mengenai peneglolaan perkembangan SDM yang bertujuan untuk mencegah terjadinya risiko dengan penyebab kondisi SDM kurang berkompeten.

		Kebijakan ini berkaitan dengan SOP pelatihan dan pengembangan yang dibuat berdasarkan standar ISO 27001:2013 pada klausul A.7.2.2.
KB-ICT-04	Kebijakan Pengelolaan Peralatan	Pedoman mengenai pengelolaan peralatan TI yang bertujuan untuk meminimalisasi terjadinya risiko kerusakan pada peralatan TI. Kebijakan ini ini dibuat berdasarkan standar ISO 27001:2013 pada klausul A.11.2.3 dan A.11.2.4.
KB-ICT-05	Kebijakan Keamanan Jaringan	Pedoman mengenai pengelolaan penggunaan jaringan yang bertujuan untuk mencegah terjadinya risiko keamanan informasi. Kebijakan ini ini dibuat berdasarkan standar ISO 27001:2013 pada klausul A.9.1.2, A.13.1.1, dan A.13.1.2.
SOP-ICT-01	SOP Klasifikasi Informasi	Merupakan prosedur yang berfungsi sebagai pedoman dalam klasifikasi informasi. Prosedur ini dibuat untuk memudahkan pencarian informasi jika dibutuhkan. Dalam prosedur ini terdapat dokumen yang dibutuhkan yakni formulir daftar informasi. dengan tambahan refrensi dari standar ISO 27017:2015 pada kontrol 12.4.1 untuk panduan dalam implementasi *cloud.*
SOP-ICT-02	SOP B*ackup* dan *Restore*	Merupakan prosedur yang berfungsi untuk menetapkan bahwa kegiatan *backup* harus dilakukan secara berkala sesuai ketentuan dan keutuhan informasi selama proses *backup* dan *restore* dilakukan. Prosedur ini diusulkan untuk selalu menjaga ketersediaan informasi saat dibutuhkan. Dalam prosedur ini terdapat dokumen yang dibutuhkan yakni formulir klasifikasi informasi serta *log backup* dan *restore* dengan tambahan refrensi dari standar ISO 27017:2015 pada kontrol 12.3.1 untuk panduan dalam implementasi *cloud.*
SOP-ICT-03	SOP Pengelolaan P*asword*	Merupakan prosedur yang berfungsi untuk menetapkan pengelolaan pada *password* serta memastikan *password pengguna* telah memenuhi kriteria *strong password.* Prosedur ini diusulkan untuk meminimalisasi ancaman manipulasi data maupun pencuriaan data yang disebabkan oleh username dan password yang diketahui orang lain. Dalam prosedur ini terdapat dokumen yang dibutuhkan yakni formulir *reset password* dan pergantian
		password
SOP-ICT-04	SOP Pengelolaan M*alware*	Merupakan prosedur yang berfungsi untuk mengelola pencegahan terhadap bahaya *malware* terhadap aset. Prosedur ini diusulkan untuk mencegah ancaman kehilangan data akibat *virus* dan *malware.* Dalam prosedur ini terdapat dokumen yang dibutuhkan yakni formulir laporan gangguan keamanan informasi.
SOP-ICT-05	SOP Pertukaran Informasi	Merupakan prosedur yang berfungsi sebagai pedoman dalam pertukaran informasi yang dilakukan dalam *mail server.* Dalam prosedur ini terdapat dokumen yang dibutuhkan yakni formulir *log* pertukaran informasi
SOP-ICT-06	SOP Pengelolaan Hak Akses	Merupakan prosedur yang berfungsi sebagai pedoman dalam pengelolaan hak akses. Prosedur ini diusulkan untuk mencegah adanya akses ilegal yang dapat menyebabkan kerugian oleh pihak yang tidak bertanggung jawab. Dalam prosedur ini terdapat dokumen yang dibutuhkan yakni formulir pengelolaan hak akses dan *log* pengelolaan hak akses dengan tambahan refrensi dari standar ISO 27017:2015 pada kontrol 9.2.3 dan 9.2.4 untuk panduan dalam implementasi *cloud.*
SOP-ICT-07	SOP Pelatihan dan Pengembangan SDM	Merupakan prosedur yang berfungsi untuk mengatur pelatihan dan pengembangan kompetensi SDM. Prosedur ini diusulkan untuk meningkatkan kompetensi pegawai sehingga dapat meminimalisasi ancaman terjadinya risiko akibat SDM yang kurang kompeten. Dalam prosedur ini terdapat dokumen yang dibutuhkan yakni formulir kehadiran pegawai, permintaan pelatihan dan pengembangan serta evaluasi pelatihan dan pengembangan.
SOP-ICT-08	SOP Keamanan Kabel	Merupakan prosedur yang berfungsi untuk memastikan keamanan pada seluruh kabel telekomunikasi dikelola secara terstruktur. Prosedur ini diusulkan untuk meminimalisasi kerusakan terhadap kabel. Dalam prosedur ini terdapat dokumen yang dibutuhkan yakni formulir laporan kerusakan dan pengelolaan peralatan.
SOP-ICT-09	SOP Perawatan Peralatan	Merupakan prosedur yang berfungsi sebagai pedoman dalam pengelolaan aset. Prosedur ini diusulkan untuk meminimalisasi kerusakan terhadap aset. Dalam prosedur ini terdapat dokumen yang dibutuhkan yakni formulir

		laporan kerusakan, pemeliharaan pealatan dan pengelolaan peralatan.
SOP-ICT-10	SOP Pengelolaan Jaringan	Merupakan prosedur yang berfungsi sebagai pedoman dalam pengelolaan jaringan. Prosedur ini diusulkan untuk mencegah terjadinya risiko keamanan informasi pada jaringan. Dalam prosedur ini terdapat dokumen yang dibutuhkan yakni formulir laporan gangguan jaringan.

IV. KESIMPULAN

Dalam penerapan *cloud* computing terdapat berbagai macam ancaman yang mengancam keamanan informasi. Namun, ancaman tersebut dapat ditanggulangi dengan perencanaan tata kelola keamanan informasi yang baik sehingga dapat mencegah maupun mengatasi ancaman yang terjadi. Pada penelitian ini perencanaan tata kelola keamanan informasi dalam penerapan *cloud* computing dibuat berdasarkan SNI ISO/IEC 27001:2013 dengan menggunakan metode OCTAVE melalui pendekatan evaluasi risiko dari 3 aspek keamanan informasi yakni *confidentially, integrity* dan *avaibility (CIA)*. Tahapan proses yang dilakukan dengan metode tersebut antara lain identifikasi aset yang menghasilkan daftar dan nilai aset, identifikasi ancaman yang menghasilkan daftar dan nilai ancaman pada aset, identifikasi nilai bisnis yang menghasilkan daftar dampak dan nilai BIA pada aset, Identifikasi nilai dan level risiko yang menunjukkan nilai serta klasifikasi level risiko pada aset. Berdasarkan proses tersebut dapat dilihat bahwa risiko pada masing-masing aset dengan nilai tertinggi terdapat pada aset informasi yakni laporan keuangan. Setelah mengetahui nilai dan level risiko dilakukan pemilihan penanganan pada masing-masing risiko. Dimana pilihan penangan yakni, penerimaan dan pengelolaan pada risiko yang mengacu pada ISO 27001:2013, proses selanjutnya yakni melakukan usulan perencanaan kebijakan dan prosedur yang digunakan sebagai upaya untuk menjaga keamanan informasi dalam penerapan *cloud computing.* Berdasarkan proses yang telah dilakukan dalam penelitian didapatkan usulan perancangan 5 kebijakan (kebijakan keamanan informasi, kebijakan pengendalian hak akses, kebijakan pengembangan SDM, kebijakan pengelolaan peralatan, dan kebijakan pengelolaan jaringan) serta 10 SOP (SOP Klasifikasi Informasi, SOP B*ackup* dan R*estore,* SOP Pengelolaan P*asword,* SOP Pengelolaan M*alware,* SOP Pertukaran Informasi, SOP Pengelolaan Hak Akses, SOP Pelatihan dan Pengembangan SDM, SOP Keamanan Kabel, SOP Perawatan Peralatan dan SOP Pengelolaan Jaringan).

UCAPAN TERIMA KASIH

Penulis memanjatkan puji syukur terhadap kehadirat Allah SWT, karena atas segala rahmat dan hidayah-Nya pembuatan artikel ini dapat diselesaikan dengan baik. Penulis juga sangat berterimakasih terhadap dosen pembimbing serta orang-orang terdekat atas bantuan, dukungan serta bimbingan selama penyusunan artikel ini dilakukan.

REFRENSI

[1] (2008) PT Steel Pipe Industry of Indonesia, Tbk website *(online), https://steelindonesia.com/company,* tanggal akses: 23 Januari 2021.

[2] Desmira. Sumarno, Dwi. Yuliani, Ririn. "Rancang Bangun *Mail Server* Berbasis *Squirrelmail* Menggunakan MTA *(Mail Transfer Agent)* pada PT.Teras Inti Media". *Jurnal PROSISKO.* Vol:4 (2): hal. 55-56, 2017.

[3] Ismail, Syed dan Asha. "Security Issues and Solutions in Cloud Computing A Survey". *International Journal of Computer Science and Information Security (IJCSIS),* Vol.14 (5), 2016.

[4] Lenawati, Mei. Winarto, Wing Wahyu. Amborowati, Armadyah. "Tata Kelola Keamanan Informasi pada PDAM Menggunakan ISO 27001:2013 dan COBIT 5*". Jurnal Sentra Penelitian Engineering dan Edukai (Speed),* Vol. 9 (1), 2017.

[5] Maulana, M. M. *Audit Keamanan Sistem Informasi Pada Dinas Komunikasi dan Informatika Kabupaten Bogor Menggunakan Standar ISO/IEC 27001:2013 dan COBIT 5*. Jakarta: Universitas Islam Negeri Syarif Hidayatullah. 2019.

[6] Direktorat Keamanan Informasi. *Panduan Penerapan Sistem Manajemen Keamanan Informasi Berbasi Indeks Keamanan Informasi (KAMI)*. Jakarta: Penerbit Kementrian Komunikasi dan Informatika. 2017.

[7] ISO/IEC 27001:2013. *Information Technology- Security Techniques-Information Security Management System-Requirements. (ebook).*

[8] Gulo, W. *Metode Penelitian*. Jakarta: PT. Grasindo. 2002.

[9] Alberts, Christopher and Dorofee, Audrey. *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE).* Pittssburgh, PA: Software Engineering Institute, Carnegie Mellon University. 2001.

[10] Sarno, R. dan I. Iffano. *Sistem Manajemen Keamanan Informasi*. Surabaya: Itspress. 2009

[11] ISO/IEC 27001:2013. *Information Technology- Security Techniques* - Codes of practice for information security controls. *(ebook).*