JURNAL TEKNOINFO
Volume 16, Nomor 2, Juli 2022, Page 165-182
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

EVALUASI RISIKO KEAMANAN INFORMASI DISKOMINFO PROVINSI XYZ MENGGUNAKAN INDEKS KAMI DAN ISO 27005 : 2011

I Putu Setyo Syahindra[1)], Clara Hetty Primasari*[2)], Aloysius Bagas Pradipta Irianto[3)]

[1,2,3]Program Studi Sistem Informasi, Universitas Atma Jaya Yogyakarta
[1,2,3]Jl. Babarsari No. 43 Yogyakarta, Indonesia
Email: [1]ptsetyo@gmail.com, [2]clara.hetty@uajy.ac.id,[3]bagas.pradipta@uajy.ac.id

Abstract

In the process of implementing information technology governance in an agency, security is a very important aspect to protect assets from all forms of threats. It is also important for agencies to evaluate the level of security that has been implemented. XYZ Province Diskominfo is a government agency that utilizes information technology in carrying out its business processes. The business process is the main asset for the agency that must be protected. The agency has implemented information security and carried out an evaluation. However, the results show that there are still weaknesses, especially on the risk side. The agency has not yet implemented information security risk management. This causes frequent internal and external incidents to occur. The government has made efforts to issue regulations regarding the implementation of information security governance for public administrators, including the XYZ Province Diskominfo, to use the ISO 27000 series. Therefore, through this research by analyzing the results of the Kami Index assessment which is the implementation of SNI ISO/IEC 27001. Then followed by risk management using ISO/IEC 27005: 2011 to find out how the risks arise from the safeguards that have been implemented. The final result of this research is to determine the level of readiness of information security that has been implemented by the agency and to make improvement strategies for information security management in order to improve the quality of service to each stakeholder.

Keyword: *KAMI Index, SNI ISO/IEC 27001, ISO/IEC 27005 : 2011, Information Security, Risk management*

Abstrak

Dalam proses pelaksanaan tata kelola teknologi informasi di suatu instansi, keamanan merupakan aspek yang sangat penting untuk melindungi aset dari segala bentuk ancaman. Evaluasi juga penting dilakukan oleh instansi untuk mengetahui sejauh mana tingkat pengamanan yang sudah diterapkan. Diskominfo Provinsi XYZ merupakan instansi pemerintahan yang memanfaatkan teknologi informasi dalam melaksanakan proses bisnisnya. Proses bisnis tersebut merupakan aset utama bagi instansi yang harus dilindungi. Instansi sudah menerapkan pengamanan informasi dan melakukan evaluasi. Namun, hasilnya menunjukkan masih adanya kelemahan terutama di bagian risiko. Instansi memang belum menerapkan manajemen risiko keamanan informasi. Hal itu menyebabkan masih sering terjadinya insiden internal maupun eksternal. Pemerintah sudah berupaya dengan mengeluarkan peraturan mengenai penerapan tata kelola keamanan informasi bagi penyelenggara publik termasuk Diskominfo Provinsi XYZ untuk menggunakan seri ISO 27000. Oleh karena itu melalui penelitian ini dengan melakukan analisis terhadap hasil penilaian Indeks KAMI yang merupakan implementasi dari SNI ISO/IEC 27001. Kemudian dilanjutkan dengan pengelolaan risiko menggunakan ISO/IEC 27005 : 2011 untuk mengetahui bagaimana risiko yang timbul dari pengamanan yang sudah diterapkan. Hasil akhir dari penelitian ini adalah mengetahui tingkat kesiapan pengamanan informasi yang sudah diterapkan oleh instansi dan membuat strategi perbaikan untuk manajemen keamanan informasi guna meningkatkan kualitas layanan kepada setiap pemangku kepentingan

Kata Kunci: Indeks KAMI, SNI ISO/IEC 27001, ISO/IEC 27005 : 2011, Keamanan Informasi, Manajemen Risiko.

1. PENDAHULUAN

Keamanan adalah bagian penting dalam proses tata kelola teknologi informasi guna mengurangi celah ancaman pada aset yang meliputi kerahasiaan, keutuhan dan ketersediaannya [1]. Diskominfo Provinsi XYZ merupakan instansi pemerintahan sebagai penyelenggara sistem elektronik yang memanfaatkan teknologi informasi dalam melaksanakan proses bisnisnya. Proses bisnis tersebut merupakan aset utama bagi Diskominfo Provinsi XYZ termasuk juga dengan sub-proses dan kegiatan-kegiatan di dalamnya.

Keamanan informasi dan pelaksanaan sistem elektronik wajib menerapkan standar SNI ISO/IEC 27001 berdasarkan

JURNAL TEKNOINFO
Volume 16, Nomor 2, Juli 2022, Page 165-182
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

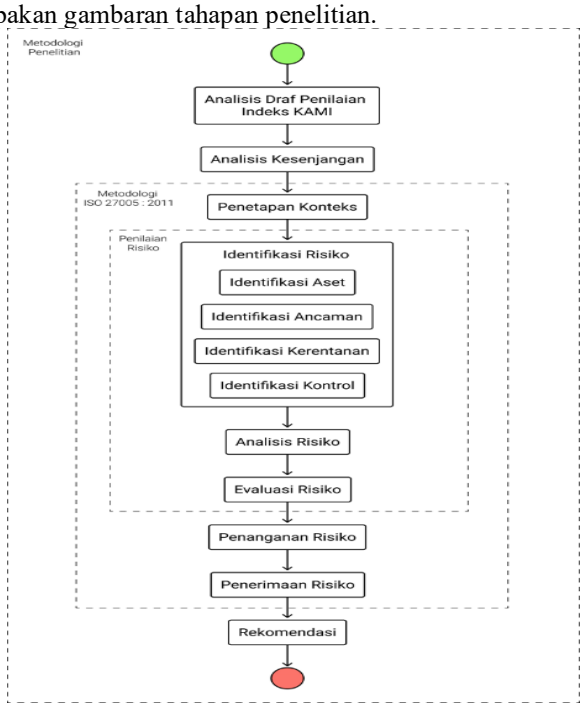
Peraturan Menteri Komunikasi dan Informatika No. 4 Tahun 2016 bahwa pengamanan informasi dilaksanakan untuk kepentingan dan pelayanan publik [2]. Evaluasi menggunakan alat bantu Indeks KAMI menggambarkan implementasi dari SNI ISO/IEC 27001:2011 pada setiap area pengamanan informasi pada instansi pemerintah [3]. Evaluasi membantu instansi untuk mengetahui keadaan dan posisinya saat ini serta menentukan target yang ingin dicapai ke depannya [4].

Pemerintah juga mengeluarkan peraturan mengenai manajemen risiko sebagai alat yang penting dalam melindungi keamanan informasi dalam instansi, sama halnya dalam Perpres No. 95 Tahun 2018 memuat bahwa keseluruhan Sistem Pemerintahan Berbasis Elektronik (SPBE) perlu meminimalisir ancaman agar pelayanan publik tetap maksimal [5]. Bagi penyelenggara publik, sangat dianjurkan dalam pengamanan informasi menggunakan seri ISO 27000 sesuai dengan Panduan Penerapan Tata Kelola Keamanan Informasi [6]. ISO/IEC 27005 adalah kerangka kerja untuk melaksanakan manajemen risiko dalam pengamanan informasi [7].

Evaluasi instansi di tahun terakhir menggunakan Indeks KAMI di bagian risiko masih sangat rendah. Instansi belum melakukan manajemen risiko keamanan informasi sehingga masih sering terjadi insiden seperti kerusakan dokumen, serangan *ransomware* dan lainnya. Hal tersebut dapat menyebabkan terganggunya kinerja pelayanan pemerintah, menurunnya reputasi pemerintah, hilangnya kepercayaan masyarakat terhadap layanan pemerintah dan sebagainya. Maka, dibutuhkan pengelolaan terhadap risiko keamanan informasi secara efektif guna mencegah atau mengurangi terjadinya dampak insiden yang lebih merugikan lagi [8].

2. METODE PENELITIAN

Penelitian ini menggunakan metode deskriptif kualitatif dari Indeks KAMI dan juga ISO 27005 : 2011. Data yang diperoleh berasal dari kuesioner, wawancara tidak terstruktur, dan studi dokumen instansi maupun penelitian sebelumnya. Pada Gambar 1 berikut ini merupakan gambaran tahapan penelitian.



Gambar 1. Tahapan penelitian

2.1 Indeks Keamanan Informasi (KAMI)

Indeks Keamanan Informasi (KAMI) adalah alat bantu dalam melaksanakan penilaian pada tingkat kesiapan yang memuat kelengkapan dan kematangan pengamanan informasi berlandaskan pada SNI ISO/IEC 27001 pada area Tata Kelola Keamanan Informasi, Pengelolaan Risiko Keamanan Informasi, Kerangka Kerja Keamanan Informasi, Pengelolaan Aset Informasi, Teknologi dan Keamanan Informasi, dan Suplemen [10].

Kategori Sistem Elektronik terdiri dari 3 kategori yaitu rendah, tinggi, dan strategis. Kategori tingkat ketergantungan dapat dilihat secara detail pada Tabel 1.

JURNAL TEKNOINFO
Volume 16, Nomor 2, Juli 2022, Page 165-182
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

Tabel 1. Kategori tingkat ketergantungan

Kategori Sistem Elektronik				
Rendah		Skor Akhir		Status Kesiapan
10	15	0	174	Tidak layak
		175	312	Pemenuhan kerangka kerja dasar
		313	535	Cukup baik
		536	645	Baik
Tinggi		Skor Akhir		Status Kesiapan
16	34	0	272	Tidak layak
		273	455	Pemenuhan kerangka kerja dasar
		456	583	Cukup baik
		584	645	Baik
Strategis		Skor Akhir		Status Kesiapan
35	50	0	333	Tidak layak
		334	535	Pemenuhan kerangka kerja dasar
		536	609	Cukup baik
		610	645	Baik

Setiap area berisikan tingkat kematangan, kategori pengamanan, daftar pertanyaan, status penerapan, dan skor. Setiap pilihan jawaban memiliki bobot penilaian seperti pada Tabel 2.

Tabel 2. Bobot penilaian status penerapan

	Kategori Pengamanan		
Status Pengamanan	1	2	3
Tidak dilakukan	0	0	0
Dalam perencanaan	1	2	3
Dalam penerapan atau diterapkan sebagian	2	4	6
Diterapkan secara menyeluruh	3	6	9

Pada Tabel 3 merupakan jumlah pertanyaan berdasarkan kategori pengamanan yang disesuaikan dengan Tabel 2.

Tabel 3. Jumlah pertanyaan berdasarkan pengamanan dan skor maksimal

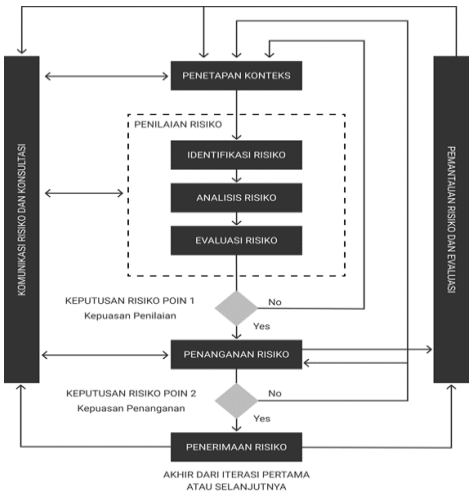
Kategori Pengamanan	Area Evaluasi					
	Tata Kelola	Risiko	Kerangka Kerja	Pengelolaan Aset	Teknologi	Suplemen
1	8	10	12	24	14	53
2	8	4	10	10	10	-
3	6	2	7	4	2	-
Skor Maksimal	126	72	159	168	120	212

Beberapa tingkat kematangan yaitu I = Kondisi awal, II = Penerapan kerangka dasar, III = Terdefinisi dan konsisten, IV = Terkelola dan terukur, dan V = Optimal. Agar mendapatkan gambaran tingkatan yang lebih rinci maka ditambahkan + dan – sehingga menjadi 9 tingkatan kematangan yaitu I, I+, II, II+, III, III+, IV, IV+, dan V. Batas minimum berdasarkan ISO 27001 adalah III+.

2.2 ISO 27005 : 2011

ISO/IEC 27005 adalah seri Sistem Manajemen Keamanan Informasi (SMKI) yang berguna sebagai acuan untuk melaksanakan manajemen risiko dalam pengamanan informasi [7]. Pada Gambar 1 adalah alur proses pengelolaan risiko dan dilanjutkan dengan penjelasannya [12].

JURNAL TEKNOINFO
Volume 16, Nomor 2, Juli 2022, Page 165-182
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index



Gambar 2. Alur proses pengelolaan risiko

1. Penetapan Konteks

   Tahap menentukan gambaran umum, kriteria dasar, ruang lingkup dan batasan dalam pelaksanaan manajemen risiko.
2. Penilaian Risiko

   Bagian ini berisikan sub-bagian yang pertama identifikasi risiko yang berisi identifikasi terhadap aset, ancaman, kerentanan, dan kontrol. Kedua adalah analisis risiko yang berisi analisis kemungkinan dan dampak terjadinya risiko menggunakan pedoman dari penelitian sebelumnya yang dilakukan oleh Asriyanik yang digambarkan pada Tabel 4 dan Tabel 5 di bawah ini [7].

Tabel 4. Kategori kemungkinan terjadinya ancaman

Kategori Kemungkinan Terjadinya Ancaman (*Likelihood*)	Penjelasan
Very Unlikely (1)	Ancaman hampir tidak pernah terjadi
Unlikely (2)	Frekuensi kejadian ancaman jarang (1 – 5 kali)
Possible (3)	Frekuensi kejadian ancaman cukup sering (6-10 kali)
Likely (4)	Frekuensi kejadian ancaman sering (10-20 kali)
Frequent (5)	Frekuensi kejadian ancaman sangat sering (>20 kali)

Tabel 5. Kategori dampak terjadinya ancaman

Kategori Dampak Terjadinya Ancaman	Penjelasan
Very Low (1)	Dampak tidak signifikan. Artinya tidak menimbulkan gangguan aktivitas yang berarti. Untuk masalah ini toleransi penyelesaian sampai 7 hari
Low (2)	Dampak gangguan kecil. Toleransi penyelesaian masalah 1-2 hari
Medium (3)	Dampak gangguan sedang. Masalah harus dapat diselesaikan paling lama 1 hari
High (4)	Dampak gangguan besar. Masalah harus dapat diselesaikan < 12 jam
Very High (5)	Dampak sangat krusial. Masalah ini harus dapat diselesaikan < 1 jam

Setelah itu, dilanjutkan dengan pelevelan risiko yang digambarkan pada Tabel 6 di bawah ini.

Tabel 6. Matriks penilaian dan level risiko

		Kemungkinan Terjadinya Ancaman (*Likelihood*)				
		Very Unlikely (1)	*Unlikely (2)*	*Possible (3)*	*Likely (4)*	*Frequent (5)*
Dampak Terjadinya	*Very Low (1)*	1/L	2/L	3/L	4/M	5/M
	Low (2)	2/L	4/L	6/M	8/M	10/M
	Medium (3)	3/L	6/M	9/M	13/M	15/H

JURNAL TEKNOINFO
Volume 16, Nomor 2, Juli 2022, Page 165-182
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

Likely (4)	4/M	8/M	12/M	16/H	20/H
Very High (5)	5/M	10/M	15/H	20/H	25/H

L = *Low*, M = *Medium*, H = *High*, Ketiga adalah evaluasi risiko untuk mendaftarkan skenario risiko berdasarkan level dan nilainya.

3. Penanganan Risiko

Berdasarkan pada panduan ISO 27005 : 2011 ada 4 opsi untuk penanganan risiko antara lain [12]. *Risk Modification* (RM) yaitu risiko harus dilakukan tindakan guna mereduksi dampak yang terjadi hingga pada nilai yang bisa diterima [12]. *Risk Retention* (RR) yaitu risiko dapat diterima atau ditahan tanpa melakukan tindakan lebih lanjut [12]. *Risk Avoidance* (RA) yaitu menghindari risiko sepenuhnya [12]. *Risk Sharing* (RS) yaitu pilihan jika biaya penanganan risiko dan dampaknya sama besar [13]. Berdasarkan pada penelitian sebelumnya yang dilakukan oleh Jonny, dkk. penanganan risiko digambarkan pada Tabel 7 berikut ini [14].

Tabel 7. Matriks penanganan risiko

Level Risiko	Biaya Pemulihan		
	Low (L)	*Medium (M)*	*High (H)*
Low (L)	*Risk Retention*	*Risk Modification*	*Risk Sharing/Avoidance*
Medium (M)	*Risk Modification*	*Risk Modification*	*Risk Sharing/Avoidance*
High (H)	*Risk Avoidance*	*Risk Avoidance*	*Risk Sharing/Avoidance*
	Low (L)	*Medium (M)*	*High (H)*
	Biaya Transfer		

4. Penerimaan Risiko

Penentuan keputusan oleh pihak yang bertanggung jawab dalam penerimaan risiko di suatu instansi.

5. Konsultasi dan Komunikasi

Kegiatan untuk mencapai kesepakatan pengelolaan risiko melalui diskusi yang dilakukan oleh pihak yang terkait.

6. *Monitoring* dan Evaluasi

Risiko bersifat dinamis, oleh karena itu harus selalu dilakukan *review* dan *monitoring* terhadap peluang, ancaman dan serangan yang mungkin terjadi [7].

2.2 Aset Teknologi Informasi

Aset pada sistem informasi tidak hanya *hardware* dan *software* tapi berupa *information, processes* dan *systems* [15]. Sesuai dengan yang termuat pada pedoman ISO 27005 : 2011, aset dapat dibagi menjadi dua jenis yaitu aset utama dan aset pendukung [12]. Aset Utama terdiri dari proses bisnis yang merupakan proses bisnis instansi termasuk juga dengan sub-proses dan kegiatan-kegiatan di dalamnya [12] dan informasi yang mencangkup informasi sebagai hal yang penting bagi suatu instansi. Sedangkan aset pendukung terdiri dari perangkat keras, perangkat lunak, jaringan, personel, situs, dan organisasi.

3. HASIL DAN PEMBAHASAN

3.1. Analisis Draf Penilaian Indeks KAMI

3.1.1. Kategori Sistem Elektronik

Dalam tahapan Kategori Sistem Elektronik, rekapitulasi nilai yang diperoleh pada Tabel 8 berikut ini.

Tabel 8. Rekapitulasi nilai kategori sistem elektronik

Status Penilaian	Bobot Nilai	Hasil Responden (Total 10 Pertanyaan)	Jumlah
A	5	4	20
B	2	5	10
C	1	1	1

JURNAL TEKNOINFO
Volume 16, Nomor 2, Juli 2022, Page 165-182
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

Total Skor	31

Berdasarkan pada hasil evaluasi yang termuat pada Tabel 8 skor sebesar 31 dapat digolongkan dalam kategori tinggi.

3.1.2. Tata Kelola Keamanan Informasi

Rekapitulasi nilai yang diperoleh terkait tata kelola pada Tabel 9 berikut ini.

Tabel 9. Rekapitulasi nilai area tata kelola keamanan informasi

Status Penerapan	Kategori Pengamanan (KP) 1		2		3		Jumlah
	Bobot Nilai	Skor Responden	Bobot Nilai	Skor Responden	Bobot Nilai	Skor Responden	
Tidak dilakukan	0	0	0	0	0	0	0
Dalam perencanaan	1	0	2	0	3	0	0
Dalam penerapan atau diterapkan sebagian	2	0	4	1	6	1	10
Diterapkan secara menyeluruh	3	8	6	7	9	5	111
Total Skor Area Tata Kelola Keamanan Informasi							121

Dari Tabel 9 di atas, instansi memperoleh total skor pada area Tata Kelola Keamanan Informasi sebesar 121. Dengan nilai tersebut persentase pemenuhan sebesar 96% dari nilai maksimal. Berdasarkan *tools*, area ini memperoleh Tingkat Kematangan yaitu III+.

3.1.3. Pengelolaan Risiko Keamanan Informasi

Rekapitulasi nilai yang diperoleh terkait pengelolaan risiko pada Tabel 10 berikut ini.

Tabel 10. Rekapitulasi nilai area pengelolaan risiko keamanan informasi

Status Penerapan	Kategori Pengamanan (KP) 1		2		3		Jumlah
	Bobot Nilai	Skor Responden	Bobot Nilai	Skor Responden	Bobot Nilai	Skor Responden	
Tidak dilakukan	0	0	0	0	0	2	0
Dalam perencanaan	1	3	2	2	3	0	7
Dalam penerapan atau diterapkan sebagian	2	6	4	2	6	0	20
Diterapkan secara menyeluruh	3	1	6	0	9	0	3
Total Skor Area Pengelolaan Risiko Keamanan Informasi							30

Dari Tabel 10 di atas, instansi memperoleh total skor untuk area Pengelolaan Risiko Keamanan Informasi sebesar 30. Dengan nilai tersebut persentase pemenuhan sebesar 41,6% dari nilai maksimal. Berdasarkan *tools*, area ini memperoleh Tingkat Kematangan yaitu I+.

3.1.4. Kerangka Kerja Pengelolaan Keamanan Informasi

Pada bagian kerangka kerja, rekapitulasi nilai yang diperoleh pada Tabel 11 berikut ini.

Tabel 11. Rekapitulasi nilai area kerangka kerja

Status Penerapan	Kategori Pengamanan (KP) 1		2		3		Jumlah
	Bobot Nilai	Skor Responden	Bobot Nilai	Skor Responden	Bobot Nilai	Skor Responden	
Tidak dilakukan	0	2	0	4	0	7	0
Dalam perencanaan	1	0	2	0	3	0	0

JURNAL TEKNOINFO
Volume 16, Nomor 2, Juli 2022, Page 165-182
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

Dalam penerapan atau diterapkan sebagian	2	2	4	2	6	0	12
Diterapkan secara menyeluruh	3	8	6	4	9	0	48
Total Skor Area Kerangka Kerja Pengelolaan Keamanan Informasi							60

Dari Tabel 11 di atas, instansi memperoleh total skor untuk area Kerangka Kerja Pengelolaan Keamanan Informasi sebesar 60. Dengan nilai tersebut persentase pemenuhan sebesar 37,7% dari nilai maksimal. Berdasarkan *tools*, area ini memperoleh Tingkat Kematangan yaitu I+.

3.1.5. Pengelolaan Aset Informasi

Rekapitulasi nilai yang diperoleh dalam pengelolaan aset pada Tabel 12 berikut ini.

Tabel 12. Rekapitulasi nilai area pengelolaan aset informasi

Status Penerapan	Kategori Pengamanan (KP) 1		2		3		Jumlah
	Bobot Nilai	Skor Responden	Bobot Nilai	Skor Responden	Bobot Nilai	Skor Responden	
Tidak dilakukan	0	0	0	0	0	1	0
Dalam perencanaan	1	0	2	1	3	0	2
Dalam penerapan atau diterapkan sebagian	2	9	4	1	6	0	22
Diterapkan secara menyeluruh	3	15	6	8	9	3	120
Total Skor Area Pengelolaan Aset Informasi							144

Dari Tabel 12 di atas, instansi memperoleh total skor untuk area Pengelolaan Aset Informasi sebesar 144. Dengan nilai tersebut persentase pemenuhan sebesar 85,7% dari nilai maksimal. Berdasarkan *tools*, area ini memperoleh Tingkat Kematangan yaitu III.

3.1.6. Teknologi dan Keamanan Informasi

Rekapitulasi nilai yang diperoleh terkait teknologi pada Tabel 13 berikut ini.

Tabel 13. Rekapitulasi nilai area teknologi dan keamanan informasi

Status Penerapan	Kategori Pengamanan (KP) 1		2		3		Jumlah
	Bobot Nilai	Skor Responden	Bobot Nilai	Skor Responden	Bobot Nilai	Skor Responden	
Tidak dilakukan	0	0	0	1	0	0	0
Dalam perencanaan	1	0	2	0	3	0	0
Dalam penerapan atau diterapkan sebagian	2	4	4	4	6	0	24
Diterapkan secara menyeluruh	3	10	6	5	9	2	78
Total Skor Area Teknologi dan Keamanan Informasi							102

Dari Tabel 13 di atas, instansi memperoleh total skor untuk area Teknologi dan Keamanan Informasi sebesar 102. Dengan nilai tersebut persentase pemenuhan sebesar 85% dari nilai maksimal. Berdasarkan *tools*, area ini memperoleh Tingkat Kematangan yaitu II+.

4.1.7. Suplemen

Pada setiap golongan memiliki jumlah pertanyaan yang berbeda-beda. Pada Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan pertanyaannya berjumlah 27. Pada Pengamanan Layanan Infrastruktur Awan (*Cloud Service*) pertanyaannya berjumlah 10. Sedangkan pada Perlindungan Data Pribadi pertanyaannya berjumlah 16. Oleh karena itu,

JURNAL TEKNOINFO
Volume 16, Nomor 2, Juli 2022, Page 165-182
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

untuk memperoleh nilai pada setiap golongan aspek pendukung bisa menerapkan rumus (1), lalu (2), dan terakhir (3).

$$Perolehan\ Nilai = 3(jumlah\ pertanyaan\ bernilai\ 3) + 2(jumlah\ pertanyaan\ bernilai\ 2) + 1(jumlah\ pertanyaan\ bernilai\ 1) \quad (1)$$

$$Skor\ Golongan = \frac{Perolehan\ Nilai}{Jumlah\ Pertanyaan} \quad (2)$$

$$Persentase\ Skor = \frac{Skor\ Golongan}{3} \times 100 \quad (3)$$

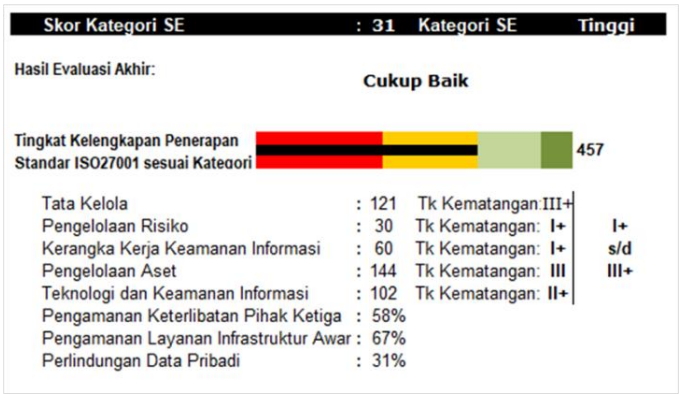
Berikut ini adalah rekap hasil evaluasi pada area Suplemen pada Tabel 14.

Tabel 14. Rekap hasil evaluasi pada area suplemen

Golongan	Perolehan Nilai	Jumlah Pertanyaan	Skor Golongan	Persentase Skor
Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan	47	27	1,74	58%
Pengamanan Layanan Infrastruktur Awan (*Cloud Service*)	20	10	2,00	67%
Perlindungan Data Pribadi	15	16	0,94	31%

3.1.7. Hasil Penilaian Indeks Kami

Setelah dilakukan pengevaluasian di semua area, pada Gambar 3 berikut ini adalah tampilan dasbor hasil penilaian.



Gambar 1. Dasbor hasil penilaian

Berdasarkan Gambar 3 bisa ditarik kesimpulan yakni Kategori Sistem Elektronik di Diskominfo Provinsi XYZ mencapai skor 31 dan sudah terkategorikan "Tinggi". Di samping itu, tingkat kelengkapan dalam pemenuhan standar ISO/IEC 27001 sebesar 457 yang sudah tergolong "Cukup Baik". Tingkat kematangan tersebut secara keseluruhan menyentuh pada III+ yang berarti hasil penilaian sudah menyentuh standar minimal yang ditetapkan sesuai dengan ISO/IEC 27001.

3.2. Analisis Kesenjangan

Melakukan perbandingan antara kondisi instansi saat ini dengan kondisi ideal berdasarkan pada Indeks KAMI dan harapan dari instansi. Pada Tabel 15 di bawah ini akan berisikan perbandingan hasil penilaian antar area pada Indeks KAMI.

Tabel 15. Perbandingan hasil setiap area penilaian

Keterangan	Tata Kelola Keamanan	Pengelolaan Risiko Keamanan	Kerangka Kerja Pengelolaan	Pengelolaan Aset Informasi	Teknologi dan Keamanan

JURNAL TEKNOINFO
Volume 16, Nomor 2, Juli 2022, Page 165-182
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

	Informasi	Informasi	Keamanan Informasi		Informasi
Skor Responden	121	30	60	144	102
Persentase Pemenuhan	96%	41,6%	37,7%	85,7%	85%
Tingkat Kematangan	III+	I+	I+	III	II+

Perbandingan antar area juga dapat dilihat dari diagram radar hasil penilaian Indeks KAMI pada Gambar 4 berikut ini.

Gambar 2. Diagram radar hasil penilaian Indeks KAMI

Pada Tabel 15 berdasarkan persentase pemenuhan dan tingkat kematangannya area Pengelolaan Risiko Keamanan Informasi berada pada tingkat terendah. Pada Gambar 4 area Risiko Keamanan Informasi belum memenuhi tingkat kepatuhan terhadap ISO 27001/SNI hanya sampai pada tingkat kerangka kerja dasar. Oleh karena itu, area Pengelolaan Risiko Keamanan Informasi menjadi fokus pada penelitian ini. Poin-poin yang belum memenuhi standar ideal berdasarkan Indeks KAMI akan dilakukan manajemen risiko. Berdasarkan penilaian, keseluruhan poin pada area tersebut akan digunakan kecuali poin 3.6.

3.3. Penetapan Konteks

3.3.1. Gambaran Umum

Pengimplementasian Undang-Undang Nomor 23 Tahun 2014 dan Peraturan Pemerintah Nomor 18 Tahun 2016 mengakibatkan terbentuknya Diskominfo Provinsi XYZ yang berkewajiban untuk menyelenggarakan kegiatan pemerintahan daerah provinsi terkait dengan persandian, statistik, komunikasi, dan informatika [16].

3.3.2. Kriteria Dasar Pendukung

Berdasarkan Pedoman Komunikasi dan Informatika Nomor 6 Tahun 2017 mengenai manajemen risiko dalam ruang lingkup kementerian komunikasi dan informatika, yang termasuk kriteria dasar antara lain [17] dampak, kemungkinan, pemeringkatan risiko, dan penerimaan risiko.

3.3.3. Ruang Lingkup dan Batasan Pengelolaan Risiko

Ruang lingkup manajemen risiko yang digunakan dalam penelitian ini adalah pada proses bisnis atau kegiatan sebagai aset utama instansi dalam melakukan pengelolaan risiko keamanan informasi yang dibatasi hanya untuk aset utama yang berkesesuaian dengan poin pertanyaan pada area Pengelolaan Risiko Keamanan Informasi dalam Indeks KAMI.

3.4. Penilaian Risiko

3.4.1. Identifikasi Risiko

1. Identifikasi Aset

   Pengklasifikasian aset ini dilakukan berdasarkan pada kesepakatan dengan pihak Diskominfo Provinsi XYZ. Daftar aset yang sudah diidentifikasi akan dimuat pada Tabel 16 berikut ini.

JURNAL TEKNOINFO
Volume 16, Nomor 2, Juli 2022, Page 165-182
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

Tabel 16. Daftar aset utama pada Diskominfo Provinsi XYZ

Kode Aset	Aset
As-1	Program kerja pengelolaan risiko keamanan informasi
As-2	Penetapan penanggung jawab manajemen risiko
As-3	Kerangka kerja manajemen risiko
As-4	Pencangkupan bagian pada kerangka kerja pengelolaan risiko
As-5	Penetapan ambang batas penerimaan risiko
As-6	Identifikasi ancaman dan kelemahan pada aset utama
As-7	Penetapan dampak kerugian pada aset utama
As-8	Pengkajian risiko keamanan informasi untuk langkah mitigasi pada aset yang ada
As-9	Penyusunan langkah mitigasi terhadap risiko yang ada
As-10	Penyusunan langkah mitigasi berdasarkan pada tingkat prioritas
As-11	Pemantauan proses berjalannya mitigasi risiko
As-12	Pengevaluasian langkah mitigasi risiko
As-13	Pengkajian langkah mitigasi
As-14	Pengkajian kerangka kerja pengelolaan risiko
As-15	Penilaian efektivitas pengamanan

2. Identifikasi Ancaman

Dalam pendataan ancaman yang mungkin terjadi sudah disesuaikan dengan kesepakatan dengan pihak Diskominfo Provinsi XYZ. Daftar ancaman yang sudah diidentifikasi akan dimuat pada Tabel 17 berikut ini.

Tabel 17. Daftar ancaman pada aset utama Diskominfo Provinsi XYZ

Kode Ancaman	Ancaman
An-1	Kegagalan program kerja
An-2	Tindakan penyangkalan
An-3	Kehilangan dokumen
An-4	Penetapan personel yang tidak tepat
An-5	Kegagalan kerangka kerja
An-6	Pencangkupan bagian yang keliru
An-7	Ambang batas yang ditetapkan tidak sesuai
An-8	Identifikasi kurang akurat
An-9	Penetapan dampak kurang sesuai
An-10	Langkah-langkah mitigasi risiko yang tidak sesuai
An-11	Langkah mitigasi yang tidak sesuai dengan risiko
An-12	Langkah mitigasi tidak sesuai dengan tingkat prioritas
An-13	Mitigasi tidak terpantau
An-14	Penyalahgunaan hak
An-15	Evaluasi tidak terukur atau subjektif
An-16	Pengkajian mitigasi tidak akurat
An-17	Tidak efektifnya pengkajian kerangka kerja
An-18	Penilaian efektivitas pengamanan tidak akurat

3. Identifikasi Kerentanan

Dalam pendataan kerentanan sudah disepakati dengan pihak Diskominfo Provinsi XYZ. Daftar kerentanan yang sudah diidentifikasi akan dimuat pada Tabel 18 berikut ini.

Tabel 18. Daftar kerentanan

Kode Aset	Kode Ancaman	Kerentanan	No. Skenario Risiko
As-1	An-1	Ketidakhadiran personel	1
		Keterbatasan sumber daya (SDM, dana, dll.)	2
		Tidak adanya izin atau anjuran khusus dari pemerintah	3
		Kurangnya pelatihan personel	4
		Komunikasi yang kurang baik antar personel	5
	An-2	Tidak adanya penugasan atau prosedur yang jelas	6
		Proses rekrutmen anggota yang tidak bagus	7
		Kurang tegasnya hukuman bagi personel yang melanggar	8

JURNAL TEKNOINFO
Volume 16, Nomor 2, Juli 2022, Page 165-182
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

	An-3	Kurangnya perlindungan secara fisik untuk dokumen	9
		Kurangnya kesadaran dan pelatihan keamanan	10
		Kesalahan atau kelalaian personel	11
		Kurangnya mekanisme pemantauan	12
		Berada di daerah rawan bencana (banjir, tsunami, dll.)	13
As-2	An-4	Tidak adanya penugasan atau prosedur yang jelas	14
		Proses rekrutmen anggota yang tidak bagus	15
As-3	An-5	Ketidaktepatan dalam memilih kerangka yang sesuai	16
		Personel kurang menguasai kerangka kerja yang digunakan	17
		Kurangnya dokumentasi dari kerangka kerja	18
As-4	An-6	Personel kurang menguasai kerangka kerja yang digunakan	19
		Personel kurang mengetahui kondisi dari instansi	20
As-5	An-7	Kurangnya analisis kondisi instansi	21
		Penetapan yang dilakukan secara subjektif tanpa pemeriksaan lapangan	22
		Kurangnya dokumentasi pendukung dalam pengambilan keputusan	23
As-6	An-8	Kurangnya kompetensi dari personel yang melakukan pengidentifikasian	24
		Tidak terklasifikasinya aset pada instansi	25
		Kurang *update* terhadap bentuk-bentuk ancaman terkini	26
		Dokumen pendukung yang kurang lengkap	27
As-7	An-9	Kurangnya analisis terhadap ancaman dan kontrol yang dimiliki oleh instansi	28
		Tim analisis yang kurang kompeten	29
		Kurang tepatnya Pengidentifikasian aset yang dimiliki oleh instansi	30
As-8	An-10	Pengkajian yang tidak sesuai dengan kerangka yang digunakan	31
		Belum jelasnya pengidentifikasian dan klasifikasi aset yang dimiliki instansi	32
		Kurangnya referensi dan dokumen pendukung dalam melakukan pengkajian	33
As-9	An-11	Personel yang kurang memahami risiko yang ada	34
		Pengategorian penilaian risiko yang belum jelas	35
As-10	An-12	Belum jelasnya pengategorian ancaman berdasarkan biaya pemulihannya	36
		Pelevelan risiko yang masih belum jelas	37
		Kesalahan personel dalam melakukan pendokumentasian	38
As-11	An-13	Kelalaian dari personel yang bertugas	39
		Kurangnya tanggung jawab keamanan informasi dalam deskripsi pekerjaan	40
	An-14	Kurangnya prosedur formal untuk hak pengawasan	41
		Kurangnya prosedur untuk menangani informasi rahasia	42
As-12	An-15	Belum adanya standar penilaian yang jelas	43
As-13	An-16	Waktu pengkajian yang tidak teratur atau tidak berkala	44
		Perubahan profil risiko yang tidak disadari oleh pihak pengkaji	45
As-14	An-17	Waktu pengkajian yang tidak teratur atau tidak berkala	46

JURNAL TEKNOINFO
Volume 16, Nomor 2, Juli 2022, Page 165-182
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

		Belum adanya standar yang jelas dari tingkat keefektifan kerangka kerja	47
		Kurangnya dokumen pendukung pengkajian	48
As-15	An-18	Kurangnya prosedur penilaian yang jelas dari instansi	49
		Kurangnya validitas tanpa pengawasan dari pihak ketiga	50

4. Identifikasi Kontrol

Dari 50 skenario risiko yang sudah diidentifikasi, hanya 7 skenario risiko yang sudah terdapat kontrolnya akan dimuat pada Tabel 19 berikut ini.

Tabel 19. Daftar kontrol yang sudah ada

No. Skenario Risiko	Penjelasan Ancaman	Kontrol yang Sudah Ada
1	Kegagalan terhadap program kerja pengelolaan risiko keamanan informasi yang dipicu oleh ketidakhadiran personel	Menerapkan sistem izin kepada atasan jika mengalami terlambat/tidak hadir agar atasan dapat menugaskan rekan yang lain untuk mengerjakan tugas yang bersangkutan
2	Kegagalan terhadap program kerja pengelolaan risiko keamanan informasi yang dipicu oleh kurangnya sumber daya yang mencangkup SDM (Sumber Daya Manusia), dana, dan lainnya	Rekrutmen PHL (Pekerja Harian Lepas) sebagai pengganti PNS (Pegawai Negeri Sipil) dengan kriteria tertentu
3	Kegagalan terhadap program kerja pengelolaan risiko keamanan informasi yang dipicu ketiadaan izin atau anjuran khusus dari pemerintah	Membuat SOP (S*tandard Operating Procedure*) atau Juknis (Petunjuk Teknis) dalam melakukan kegiatan yang belum ada izin/anjuran khusus dari pemerintah, contohnya CSIRT, *Pentest*, dan lainnya
4	Kegagalan terhadap program kerja pengelolaan risiko keamanan informasi yang dipicu oleh personel yang kurang terlatih	Membuat surat permohonan pelatihan personel kepada BSSN (Badan Siber dan Sandi Negara) sebagai instansi induk pengampu keamanan informasi
6	Tindakan penyangkalan dalam pelaksanaan program kerja pengelolaan risiko keamanan informasi yang dipicu oleh tidak adanya penugasan atau prosedur yang jelas dalam pelaksanaan program kerja	Setiap pelaksanaan kegiatan dilakukan penugasan baik secara lisan maupun tertulis oleh pimpinan
9	Kehilangan/kerusakan dokumen dalam program kerja pengelolaan risiko keamanan informasi yang dipicu oleh perlindungan secara fisik terhadap dokumen yang masih kurang	Menyediakan tempat tertentu untuk menyimpan dokumen
11	Kehilangan/kerusakan dokumen dalam program kerja pengelolaan risiko keamanan informasi yang dipicu oleh kesalahan atau kelalaian yang dilakukan oleh personel	Adanya SOP (*Standard Operating Procedure*)

3.4.2. Analisis Risiko

Melakukan penilaian kemungkinan terjadinya ancaman (*likelihood*) dan dampak terjadinya ancaman pada aset utama Diskominfo Provinsi XYZ. Berikut ini pada Tabel 20 adalah hasil penilaiannya.

Tabel 20. Penilaian kemungkinan terjadinya ancaman

Kategori Kemungkinan Terjadinya Ancaman (*Likelihood*)	No. Skenario Risiko
Very Unlikely (1)	5, 6, 8, 13, 14, 16, 26, 42, 43
Unlikely (2)	1, 2, 3, 7, 9, 12, 15, 19, 20, 21, 22, 23, 24, 27, 28, 29, 30, 31, 32, 33, 34, 36, 37, 38, 39, 40, 41, 44, 45, 46, 47, 48, 49, 50
Possible (3)	10, 11, 17, 18, 25, 35
Likely (4)	4

JURNAL TEKNOINFO
Volume 16, Nomor 2, Juli 2022, Page 165-182
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

Frequent (5)	

Sedangkan untuk penilaian dampak terjadinya risiko pada Diskominfo Provinsi XYZ sudah disesuaikan dengan tingkat penerimaan risiko pada instansi tersebut. Berikut ini pada Tabel 21 adalah hasil penilaiannya.

Tabel 21. Penilaian dampak terjadinya ancaman

Kategori Dampak Terjadinya Ancaman	No. Skenario Risiko
Very Low (1)	1, 8
Low (2)	2, 3, 5, 6, 7, 14, 15, 16, 19, 20, 21, 22, 26, 27, 28, 29, 30, 31, 32, 33, 38, 39, 40, 41, 43, 44, 45, 46, 47, 48, 49, 50
Medium (3)	9, 12, 13, 17, 18, 23, 24, 25, 34, 35, 36, 37, 42
High (4)	4, 10, 11
Very High (5)	

Berdasarkan hasil penilaian kemungkinan terjadinya ancaman (*likelihood*) pada Tabel 20 dan dampak terjadinya ancaman pada Tabel 21, maka dapat dilakukan penilaian untuk memperoleh level dari setiap risiko yang ada. Kategori level risiko tersebut antara lain *High* (H), *Medium* (M), dan *Low* (L). Berikut ini pada Tabel 22 adalah hasil penilaiannya.

Tabel 22. Level risiko pada Diskominfo Provinsi XYZ

No. Skenario Risiko	Nilai Kemungkinan Terjadinya Ancaman (*Likelihood*)	Nilai Dampak Terjadinya Ancaman	Nilai Risiko	Level Risiko
1	2	1	2	L
2	2	2	4	L
3	2	2	4	L
4	4	4	16	H
5	1	2	2	L
6	1	2	2	L
7	2	2	4	L
8	1	1	1	L
9	2	3	6	M
10	3	4	12	M
11	3	4	12	M
12	2	3	6	M
13	1	3	3	L
14	1	2	2	L
15	2	2	4	L
16	1	2	2	L
17	3	3	9	M
18	3	3	9	M
19	2	2	4	L
20	2	2	4	L
21	2	2	4	L
22	2	2	4	L
23	2	3	6	M
24	2	3	6	M
25	3	3	9	M
26	1	2	2	L
27	2	2	4	L
28	2	2	4	L
29	2	2	4	L
30	2	2	4	L
31	2	2	4	L
32	2	2	4	L
33	2	2	4	L
34	2	3	6	M
35	3	3	9	M
36	2	3	6	M
37	2	3	6	M
38	2	2	4	L
39	2	2	4	L

JURNAL TEKNOINFO
Volume 16, Nomor 2, Juli 2022, Page 165-182
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

40	2	2	4	L
41	2	2	4	L
42	1	3	3	L
43	1	2	2	L
44	2	2	4	L
45	2	2	4	L
46	2	2	4	L
47	2	2	4	L
48	2	2	4	L
49	2	2	4	L
50	2	2	4	L

3.4.3. Evaluasi Risiko

Tahap ini berisi perekapan terhadap skenario risiko yang mungkin terjadi pada konteks yang sudah ditetapkan. Berikut ini pada Tabel 23 adalah rekapitulasi skenario risiko berdasarkan pada level dan nilai risiko.

Tabel 23. Skenario risiko berdasarkan level dan nilai risiko

Level Risiko	No. Skenario Risiko
High (H)	4
Medium (M)	10, 11, 17, 18, 25, 35, 9, 12, 23, 24, 34, 36, 37
Low (L)	2, 3, 7, 15, 19, 20, 21, 22, 27, 28, 29, 30, 31, 32, 33, 38, 39, 40, 41, 44, 45, 46, 47, 48, 49, 50, 13, 42, 1, 5, 6, 14, 16, 26, 43, 8

3.5. Penanganan Risiko

Ada empat opsi dalam menanggapi risiko antara lain *Risk Modification* (RM), *Risk Retention* (RR), *Risk Avoidance* (RA), dan *Risk Sharing* (RS). Keluaran dari tahap ini berupa rencana penanganan risiko yang akan dimuat pada Tabel 24 berikut ini.

Tabel 24. Rencana penanganan risiko

No. Skenario Risiko	Level Risiko	Biaya Penanganan	Penanganan Risiko
4	H	H	RS
10	M	H	RS
11	M	H	RS
17	M	M	RM
18	M	M	RM
25	M	M	RM
35	M	M	RM
9	M	M	RM
12	M	M	RM
23	M	L	RM
24	M	L	RM
34	M	M	RM
36	M	M	RM
37	M	M	RM
2	L	H	RS
3	L	M	RM
7	L	L	RR
15	L	L	RR
19	L	L	RR
20	L	L	RR
21	L	L	RR
22	L	L	RR
27	L	L	RR
28	L	L	RR
29	L	L	RR
30	L	L	RR
31	L	M	RM
32	L	L	RR
33	L	L	RR
38	L	L	RR

JURNAL TEKNOINFO
Volume 16, Nomor 2, Juli 2022, Page 165-182
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

39	L	L	RR
40	L	L	RR
41	L	L	RR
44	L	L	RR
45	L	L	RR
46	L	L	RR
47	L	L	RR
48	L	L	RR
49	L	L	RR
50	L	L	RR
13	L	M	RM
42	L	M	RM
1	L	L	RR
5	L	L	RR
6	L	L	RR
14	L	L	RR
16	L	L	RR
26	L	L	RR
43	L	L	RR
8	L	L	RR

3.6. Penerimaan Risiko

Dari rencana penanganan risiko yang sudah diajukan kepada pihak instansi, mereka memilih untuk tidak melakukan tindakan lebih lanjut terhadap risiko dengan rekomendasi penanganan *Risk Retention* (RR) karena risiko tersebut sudah dianggap dapat ditahan atau diatasi oleh pihak instansi. Sedangkan untuk rekomendasi penanganan lainnya disetujui. Berikut ini pada Tabel 25 akan dimuat risiko yang disetujui oleh pihak Diskominfo Provinsi XYZ.

Tabel 25. Risiko yang disetujui oleh Diskominfo Provinsi XYZ

Penanganan Risiko	No. Skenario Risiko
Risk Sharing (RS)	4, 10, 11, 2
Risk Modification (RM)	17, 18, 25, 35, 9, 12, 23, 24, 34, 36, 37, 3, 31, 13, 42

3.7. Rekomendasi

Sesuai dengan pedoman metode ISO 27005 : 2011, level risiko dapat dikurangi melalui pemilihan kontrol yang dimuat secara rinci pada ISO/IEC 27002 [12]. Rekomendasi perbaikan akan dimuat pada Tabel 26 di bawah ini.

Tabel 26. Daftar rekomendasi perbaikan

No. Skenario Risiko	Kontrol ISO 27002 : 2013	Penjelasan
4	7.2.2	Semua personel memiliki pendidikan dan pelatihan yang relevan untuk fungsi pekerjaan mereka. Mengadakan pelatihan dan pendidikan berbasis kelas, pengajaran jarak jauh, melalui *website*, mandiri dan sebagainya dengan berbagai bentuk misalnya seminar atau studi mandiri. Setiap kegiatan diakhiri dengan pengujian sejauh mana pemahaman personel terhadap materi.
10	7.2.2	Semua personel memiliki kesadaran keamanan informasi untuk fungsi pekerjaan mereka. Mengadakan aktivitas untuk kesadaran seperti kampanye contohnya hari kebudayaan keamanan informasi serta menerbitkan buklet atau buletin. Bekerja sama dengan pihak ketiga untuk melatih personel.
11	7.2.1	Mewajibkan personel untuk sesuai dengan kebijakan dan prosedur yang ditetapkan instansi. Melakukan pengarahan prosedur atau kode etik personel sebelum berkegiatan oleh pihak manajemen. Menyediakan pelaporan anonim terkait pelanggaran keamanan informasi (*whistle blowing*). Mengadakan tindakan pendisiplinan pada personel yang melanggar yang menjadi motivasi atau pendorong terbentuknya kepedulian yang baik terhadap keamanan informasi. Contohnya surat pemanggilan, teguran, dan lainnya. Jika berulang terus-menerus pihak yang bersangkutan dapat dibawa kepada pihak yang berwenang untuk melakukan keputusan hukum.
17	7.2.2	Personel yang bersangkutan wajib memiliki pengetahuan terkait kerangka kerja yang digunakan pada instansi. Bekerja sama dengan pihak ketiga sumber daya untuk informasi tambahan dan nasihat tentang kerangka kerja, termasuk materi pendidikan

JURNAL TEKNOINFO
Volume 16, Nomor 2, Juli 2022, Page 165-182
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

		dan pelatihan yang lebih lanjut.
18	12.1.1	Kegiatan yang dilakukan oleh instansi harus terdokumentasi dengan baik termasuk kerangka kerja yang digunakan. Instansi wajib melakukan pendokumentasian yang berisikan petunjuk pengoperasian kerangka kerja. Membentuk tim untuk mendalami kerangka kerja ataupun berkolaborasi dengan pihak ketiga dalam kepentingan dokumentasi pada kerangka kerja yang digunakan.
25	8.1.2	Melakukan klasifikasi aset secara berkala klasifikasi tersebut harus akurat, mutakhir, konsisten dan selaras dengan aset yang ada. Klasifikasi aset instansi penting dilakukan untuk menentukan ancaman atau perlindungan yang sesuai.
35	18.1.1	Menentukan kategori untuk penilaian risiko yang digunakan oleh instansi. Kategori yang ditentukan disesuaikan dengan kerangka kerja yang digunakan sesuai dengan dokumentasinya.
9	11.1	Instansi wajib mereduksi segala bentuk gangguan terhadap dokumen yang ada. Menyediakan konstruksi bangunan yang kokoh dan ruangan harus dilindungi dengan tepat dari akses ilegal melalui kontrol seperti pemasangan alarm, kamera pengawas, dan lainnya. Wajib mengunci pintu dan jendela saat tanpa pengawasan dan perlindungan eksternal. Melakukan pencatatan buku tamu. Log pengaksesan ataupun audit harus diarsipkan dan diawasi dengan aman. Mengimplementasikan beberapa mekanisme autentikasi, termasuk kartu akses dan PIN rahasia. Menerapkan personel untuk keamanan. Pembuatan izin untuk perlengkapan fotografi, video, audio atau perekam lainnya yang berpotensi sebagai pencurian data.
12	11.2.2	Mencatat log peristiwa dan meninjaunya secara berkala. Log tersebut harus mencangkup ID pengguna, aktivitas yang dilakukan, waktu berlangsungnya, lokasi, perubahan konfigurasi data, dokumen yang diakses, dan hal-hal terkait lainnya. Jika memungkinkan, personel tidak boleh memiliki izin untuk melakukan penghapusan dan menonaktifkan log mereka ketika melakukan suatu aktivitas pada dokumen yang diakses.
23	12.1.1	Melakukan dokumentasi pada aset, program kerja, dan kegiatan lainnya yang berlangsung secara resmi oleh instansi. Dokumentasi harus disimpan dalam inventaris khusus atau yang sudah ada sebagaimana mestinya. Pendokumentasian membantu meyakinkan terhadap perlindungan efektif telah terjadi, dan mungkin juga dibutuhkan dalam kepentingan pengambilan keputusan.
24	7.2.2	Mengadakan pelatihan dan pendidikan berbasis kelas, pengajaran jarak jauh, melalui *website*, mandiri dan sebagainya dengan berbagai bentuk misalnya seminar atau studi mandiri. Jika diperlukan instansi dapat bekerja sama dengan pihak ketiga sebagai sumber daya untuk informasi tambahan dan nasihat tentang pengidentifikasian ancaman maupun kelemahan, termasuk materi pendidikan dan pelatihan terkait yang lebih lanjut.
34	7.2.2	Mengadakan kegiatan peningkatan kesadaran akan keamanan informasi seperti pengarahan, seminar, dan sebagainya. Jika diperlukan instansi dapat bekerja sama dengan pihak ketiga sebagai sumber daya untuk penasihat mengenai penentuan langkah mitigasi yang tepat.
36	18.2.1	Melakukan peninjauan independen untuk mengategorikan ancaman berdasarkan biaya pemulihannya. Individu yang melakukan tinjauan ini wajib mempunyai kemampuan dan pengalaman yang relevan. Hasil peninjauan wajib dicatat serta dilaporkan kepada manajemen. Catatan tersebut wajib disimpan.
37	18.2.1	Melakukan peninjauan independen penentuan level risiko berdasarkan kerangka kerja yang digunakan. Individu yang melakukan tinjauan ini wajib mempunyai kemampuan dan pengalaman yang relevan. Hasil peninjauan wajib dicatat serta dilaporkan kepada manajemen. Catatan tersebut wajib disimpan.
2	7.1.1	Melakukan perekrutan tenaga kerja sesuai dengan yang dibutuhkan. Undang-undang ketenagakerjaan yang secara etis diperlukan untuk memasukkan pemeriksaan latar belakang semua pelamar, harus sesuai dengan persyaratan bisnis, klasifikasi informasi yang dilihat, kemampuan untuk dimiliki, dan lainnya. Informasi tentang semua kandidat yang sedang dipertimbangkan untuk posisi dalam instansi harus dikumpulkan dan ditangani sesuai dengan undang-undang terkait. Kontrak dengan pekerja harus mencerminkan kebijakan instansi seperti melakukan perjanjian *non-disclosure*. Peran dan tanggung jawab keamanan informasi harus dikomunikasikan kepada kandidat sebelum bekerja. Instansi harus memastikan bahwa pekerja menyetujui syarat dan ketentuan yang berlaku.
3	18.1.1	Manajemen harus menentukan seluruh undang-undang dan peraturan yang berlaku bagi suatu organisasi sebagai pemenuhan syarat bisnisnya. Hal tersebut dilakukan

JURNAL TEKNOINFO
Volume 16, Nomor 2, Juli 2022, Page 165-182
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

		untuk tidak melanggar hukum, peraturan, dan kewajiban kontrak yang berlaku.
31	18.2.1	Manajemen harus memulai tinjauan independen terkait risiko keamanan informasi yang ada berdasarkan kerangka kerja yang digunakan. Kajian independen semacam itu dibutuhkan agar sesuai, berkecukupan, dan efektif untuk pendekatan organisasi dalam mengelola keamanan informasi.
13	11.1.4	Penasihat spesialis dibutuhkan untuk mengetahui cara untuk menghindar dari kerusakan yang dikarenakan oleh bencana alam seperti gempa bumi, banjir, kebakaran, tsunami, dan lainnya.
42	9.1.1	Membuat prosedur penanganan informasi rahasia. Prosedur harus memuat pembatasan akses informasi dan fasilitas pengolahannya. Prosedur wajib ditetapkan secara menyeluruh, terdokumentasikan dengan baik dan ditinjau secara berkala. Pemilik informasi wajib menetapkan aturan kontrol akses yang tepat dan batasan untuk penggunaan informasi tersebut. Berisikan pemisah peran dalam pengontrolan akses seperti meminta, memberikan, mengelola, dan mencabut akses.

4. KESIMPULAN

Diskominfo Provinsi XYZ memiliki ketergantungan yang tinggi terhadap penggunaan sistem elektronik dalam melakukan proses bisnis instansi. Tingkat kelengkapan sebesar 457 yang sudah termasuk "Cukup Baik" pada pemenuhan standar ISO/IEC 27001. Namun tingkat kematangan tersebut secara keseluruhan baru menyentuh pada III+ yang berarti hasil penilaian hanya menyentuh standar minimal yang ditetapkan sesuai dengan ISO/IEC 27001.

Untuk area Pengelolaan Risiko Keamanan Informasi yang menjadi konteks pada penelitian ini berdasarkan persentase pemenuhan dan tingkat kematangannya masih rendah. Selain itu, Jika dilihat dari tingkat penerapan yang sudah dilakukan oleh instansi area tersebut belum sampai pada tingkat kepatuhan terhadap ISO 27001/SNI.

Dari proses pengelolaan risiko pada konteks yang ditetapkan, diperoleh 50 skenario risiko. Dari seluruh skenario yang ada yang sudah disesuaikan dengan penerimaan risiko oleh pihak instansi diperoleh 19 skenario yang disetujui dan akan diberikan rekomendasi perbaikan. Di antaranya terdapat 1 skenario level *High*, 13 skenario level *Medium*, dan 5 skenario level *Low*.

DAFTAR PUSTAKA

[1] P. Diah Restu Wardani1, "Evaluasi Keamanan Informasi Pada Pti Pdam Tirta Moedal Kota Semarang Berdasarkan Indeks Keamanan Informasi Sni Iso/Iec 27001:2009," *Techno.COM*, vol. 14, no. 3, pp. 165–172, 2015.

[2] N. Arman, W. Hayuhardhika, N. Putra, and A. Rachmadi, "Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Sidoarjo menggunakan Indeks Keamanan Informasi (KAMI)," vol. 3, no. 6, pp. 5750–5755, 2019.

[3] R. Firmana, B. C. Hidayanto, and H. M. Astuti, "Penggunaan Indeks Keamanan Informasi (KAMI) Sebagai Evaluasi Keamanan Informasi Pada PT. PLN Distribusi Jatim," *J. Tek. POMITS (Publikasi Online ITS)*, vol. 1, no. 1, pp. 1–5, 2013.

[4] N. Hidayati, "Kajian Tata Kelola IT Berdasarkan Indeks Kami pada Universitas Pakuan Bogor," *J. Paradig.*, vol. 16, 2014.

[5] Perpres 95 Tahun 2018, "Sistem Pemerintahan Berbasis Elektronik," *seruyankab.go.id*, 2018.

[6] Tim Direktorat Keamanan Informasi, "Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggaea Layanan Publik," *Direktorat Keamanan Inf. Kementeri. Komun. dan Inform. RI*, 2011.

[7] A. Asriyanik and U. M. Sukabumi, "Manajemen Keamanan Informasi pada Sistem Informasi Akademik Menggunakan ISO 27005," no. August 2018, 2019.

[8] H. T. I. Driantami, Suprapto, and A. R. Perdanakusuma, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Studi kasus : Sistem Penjualan PT Matahari Department Store Cabang Malang Town Square)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 11, pp. 4991–4998, 2018.

[9] I. Afrianto, T. Suryana, and S. Sufa'atin, "Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI - SNI ISO/IEC 27001:2009," *J. Ultim. InfoSys*, vol. 6, no. 1, pp. 43–49, 2015.

[10] BSSN, "Indeks KAMI | bssn.go.id," 2019. [Online]. Available: https://bssn.go.id/indeks-kami/. [Accessed: 07-Mar-2021].

[11] A. T. Megawati, H. M. Astuti, and A. Herdiyanti, "Pengelolaan Risiko Aset Teknologi Informasi Pada Perusahaan Properti Pt Xyz , Tangerang Berdasarkan," *Semin. Nas. Sist. Inf. Indones.*, no. September, pp. 449–454, 2014.

[12] I. S. O. ISO, "IEC 27005: Information technology–security techniques–information security risk management," *Iso/Iec*, vol. 44, no. 0, 2011.

[13] B. Suanda, "Strategi Mengatasi Risiko – Manajemen Proyek Indonesia," *manajemenproyekindonesia.com*, 2013. [Online]. Available: https://manajemenproyekindonesia.com/?p=2627. [Accessed: 23-Apr-2021].

[14] J. Jonny, A. Ambarwati, and C. Darujati, "Penilaian Risiko Data Sistem Informasi Manajemen Puskesmas dan Aset Menggunakan ISO 27005," *Sistemasi*, vol. 10, no. 1, p. 1, 2021.

[15] S. Salahuddin, A. Ambarwati, and M. N. Al Azam, "Identifikasi Risiko Keamanan Informasi Menggunakan Iso 27005 Pada Sebuah Perguruan Tinggi Swasta Di Surabaya," *Semin. Nas. Sist. Inf.*, pp. 990–996, 2018.

[16] D. P. XYZ, "Profil Dinas - Dinas Komunikasi dan Informatika Provinsi XYZ." [Online]. Available: https://diskominfo.xyz.go.id/2019/profil-dinas/. [Accessed: 12-Apr-2021].

[17] Mentri KOMINFO RI, "Pedoman Menteri No 6 Tahun 2017 Manajemen Risiko di Lingkungan Kemkominfo." Jaringan Dokumentasi dan Informasi Hukum (JDIH), 2017.