BRAHMANA: Jurnal Penerapan Kecerdasan Buatan
Terakreditasi Nomor 204/E/KPT/2022 | Vol. 6, No. 1, Desember (2024), pp. 16-24

Pengukuran Risiko Indeks Keamanan Informasi(Kami) Bagian Tata Kelola Kota XYZ Menggunakan *Framework Nist Sp* 800-30

I Gede Putu Krisna Juliharta[1], *Adrian*[2], *Ayu Pradnyandari Dananjaya Erawan*[3]
[1,2,3]*Universitas Primakara, Bali, Indonesia*
Email: krisna@primakara.ac.id[1], *franciskusasiang@gmail.com*[2], *ayu13pradnyandari@gmail.com*[3]

Abstract

The XYZ City Government has conducted an assessment using the KAMI Index, revealing that the governance aspect is weaker compared to other areas. Given this issue, a risk assessment was conducted to provide recommendations for the City of XYZ to improve its information security. The risk assessment was carried out using the NIST SP 800-30 framework, designed as a guideline for evaluating risk management. There are five risk categories: Very Low, Low, Moderate, High, and Very High. Based on the assessment using NIST 800-30, several critical areas for improvement were identified: Policy with a High level of risk, Data and Information with a Very High level of risk, Information Security Education with a Moderate level of risk, Accountability with a High level of risk, Implemented Programs with a High level of risk, Legal Aspects with a High level of risk, BCP and DRP Implementation with a High level of risk, Information Security Standards and Performance with a Moderate level of risk, and Information Security Management with a High level of risk.

Keywords: *Information Technology Security, Risk Assessment, NIST SP 800-30, Kami Index, Governance*

Abstrak

Pemerintah Kota XYZ telah melakukan penilaian dengan Indeks KAMI, dengan hasil bagian Tata Kelola yang kurang baik dibandingkan aspek lainnya. Dengan permasalahan ini, dilakukanlah pengukuran risiko yang berguna sebagai bahan rekomendasi atau referensi untuk Kota XYZ dalam memperbaiki dan meningkatkan keamanan informasi. Pengukuran risiko dilakukan dengan kerangka kerja NIST SP 800-30 yang dirancang sebagai panduan dalam menilai manajemen risiko. Terdapat lima kategori risiko yaitu Very Low, Low, Moderate, High, dan Very High. Berdasarkan hasil pengukuran menggunakan NIST 800-30 didapatkan beberapa aspek yang penting untuk diperbaiki yaitu Kebijakan dengan level High, Data dan Informasi dengan level Very High, Edukasi Keamanan Informasi dengan level Moderate, Penanggung Jawab dengan level High, Program yang Dilaksanakan dengan level High, Aspek Hukum dengan level High, Penerapan BCP dan DRP dengan level High, Standar Keamanan Informasi dan Kinerja dengan level Moderate dan Pengelolaan Keamanan Informasi dengan level High.

Kata kunci*: Keamanan Teknologi Informasi, Pengukuran Risiko, NIST SP 800-30, Indeks KAMI, Tata Kelola*

1. Pendahuluan

Pemerintah Kota XYZ menggunakan berbagai sistem teknologi informasi dalam melakukan pelayanan publik dan efisiensi pemerintahan. Penggunaan teknologi informasi (TI) dalam mendukung pemerintahan ini mengundang berbagai ancaman yang dapat merusak dan mengganggu sistem yang berjalan [1]. Pentingnya aspek keamanan teknologi informasi ini bertujuan untuk mengantisipasi ancaman serta risiko dari berbagai permasalahan seperti bencana alam, tidak melakukan *backup data*, infrastruktur yang buruk, serangan *hacker*, dan lain sebagainya, sehingga dengan adanya pengamanan yang baik maka akan mengurangi berbagai risiko yang mungkin akan terjadi [2].

ISSN: 2715-9906

Pemerintah Kota XYZ telah menerapkan serta mengelola berbagai macam hal yang mendukung aspek keamanan teknologi informasi, hal ini didukung dengan telah dilakukannya penilaian Indeks KAMI(Keamanan Informasi). Indeks KAMI merupakan alat ukur yang digunakan untuk menilai tingkat kematangan sistem pemerintahan di suatu instansi pemerintah [3]. Indeks KAMI ini berdasarkan dari *framework* atau kerangka kerja SNI ISO/IEC 27001 yang merupakan kerangka kerja yang berisi standar untuk melindungi sistem informasi di suatu organisasi ataupun pemerintahan. Hasil dari penilaian Indeks KAMI terhadap Kota XYZ, didapati hasil evaluasi akhir adalah Cukup Baik, akan tetapi dari beberapa faktor, terdapat satu faktor yang nilainya cukup kecil yaitu bagian Tata Kelola. Rendahnya nilai pada Tata Kelola, merupakan tantangan bagi pihak Kota XYZ dalam memperbaiki beberapa hal yang berakitan dengan Tata Kelola, agar mendapatkan nilai yang lebih baik pada penilaian Indeks KAMI dan keamanan menjadi lebih baik.

Perbaikan dari bagian Tata Kelola Indeks KAMI dapat dikembangkan dan diperbaiki dengan menggunakan kerangka kerja lain seperti NIST SP 800-30. NIST atau *National Institute of Standards and Technology* merupakan sebuah lembaga milik Amerika Serikat yang bertugas dan bertanggung jawab untuk mengembangkan standar, pedoman dan praktik terbaik untuk permasalahan terkait teknologi informasi, keamanan siber, dan komputer sains, sedangkan SP 800-30 merupakan serial dokumen yang membahas mengenai manajemen resiko untuk teknologi informasi dan sistem [4]. Kerangka kerja NIST SP 800-30 ini berisi berbagai macam pedoman dan praktik yang dapat dipraktikan untuk menilai risiko yang dimiliki oleh perusahaan atau organisasi.

Berdasarkan uraian diatas, penulis melakukan penilaian manajemen risiko menggunakan kerangka kerja NIST 800-30 dari Indeks KAMI untuk bagian Tata Kelola Kota XYZ yang berguna sebagai penilaian, evaluasi, dan bahan rekomendasi untu Kota XYZ dalam meningkatkan aspek keamanan.

2. Metodologi Penelitian

2.1. Risk Assessment

Risk Assessment (Penilaian Risiko) dalam keamanan siber adalah proses sistematis untuk mengidentifikasi, menganalisis, dan mengevaluasi risiko yang terkait dengan keamanan informasi dalam suatu organisasi. Tujuan utama dari risk assessment adalah untuk memahami potensi ancaman, kerentanan, dan dampak yang dapat mempengaruhi aset informasi, sehingga organisasi dapat mengambil langkah-langkah yang tepat untuk mengelola dan mengurangi risiko tersebut.. Ini mencakup aspek teknis dan non-teknis yang bertujuan untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi [5].

2.2. Indeks KAMI

Indeks KAMI (Keamanan Informasi) bertujuan untuk menilai atau mengukur mengenai keamanan informasi yang dimiliki oleh pemerintahan ataupun organisasi dengan kriteria berdasarkan kerangka kerja SNI ISO/IEC 270001. Terdapat beberapa aspek yang dinilai dalam Indeks KAMI, diantaranya Kategori Sistem Elektronik yang digunakan, Tata Kelola Keamanan Informasi, Pengelolaan Risiko Keamanan Informasi, Kerangka Kerja Keamanan Informasi, Pengelolaan Aset, Teknologi dan Keamanan Informasi, dan Suplemen (tambahan lainnya seperti penggunaan *cloud*) [6].

2.3. NIST SP 800-30

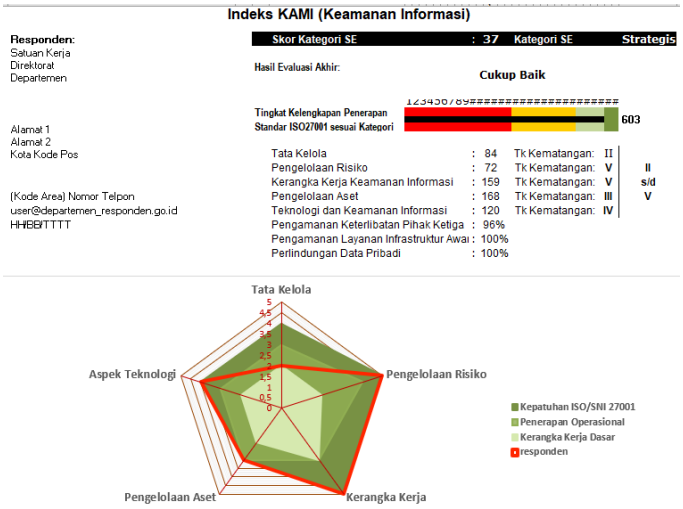
NIST SP 800-30 bertujuan untuk membantu organisasi mengelola dan memanajemen risiko keamanan informasi secara efektif dengan memberikan kerangka kerja yang terstruktur dan terstandardisasi mengenai. Dengan demikian, organisasi dapat melindungi aset informasi mereka dari berbagai ancaman dan memastikan kontinuitas operasional mereka. Terdapat beberapa tahapan dalam melakukan analisis yang dijelaskan sebagai berikut [7]:

a. *Assets Identification*, proses mengidentifikasi semua aset penting dalam organisasi yang perlu dilindungi. Aset dapat berupa data, perangkat keras, perangkat lunak, infrastruktur jaringan, dan sumber daya manusia.
b. *Threat Sources*, Sumber ancaman adalah entitas atau kondisi yang memiliki potensi untuk menyebabkan kerusakan pada aset. Sumber ancaman bisa berasal dari orang dalam (internal) seperti karyawan, orang luar (eksternal) seperti peretas, atau bahkan faktor lingkungan seperti bencana alam.
c. *Threat Event*, adalah kejadian spesifik yang dapat mengeksploitasi kerentanan dalam suatu sistem atau aset. Contohnya termasuk serangan *malware*, dan pencurian data,
d. *Vulnerabilities*, adalah kelemahan atau celah dalam sistem informasi atau proses yang dapat dieksploitasi oleh sumber ancaman untuk menyebabkan kerugian.
e. *Likelihood*, adalah penilaian tentang seberapa besar kemungkinan suatu ancaman akan mengeksploitasi kerentanan yang ada.
f. *Impact*, adalah sejauh mana konsekuensi negatif yang timbul jika suatu ancaman berhasil mengeksploitasi kerentanan
g. *Risk Determination*, adalah proses menggabungkan kemungkinan dan dampak untuk menilai tingkat risiko keseluruhan.

3. Hasil dan Pembahasan

3.1. Penilaian Indeks KAMI

Pengukuran dengan menggunakan Indeks KAMI dapat dilihat pada gambar berikut:



Gambar 1. Hasil Indeks KAMI Kota XYZ

Secara keseluruhan, hasil evaluasi yang didapatkan adalah cukup baik. Akan tetapi, pada bagian Tata Kelola didapatkan skor penilaian sebesar 84 dari 126 dengan hasil dikategorikan pada tingkat kematangan II yang berarti "Penerapan Kerangka Kerja Dasar". Tingkat kematangan dibagi menjadi lima yaitu, Bagian Tata Kelola ini merupakan bagian dengan nilai yang paling kecil daripada lainnya sehingga diperlukan peninjauan kembali sebagai bahan untuk meningkatkan dan memperbaiki bagian Tata Kelola. Penilaian Tata Kelola dapat dilihat dari jawaban pada tabel berikut :

Tabel 1. Hasil Penilaian Bagian Tata Kelola

No	Pertanyaan	Status	Skor
1	Apakah pimpinan instansi/perusahaan anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	Dalam Penerapan / Diterapkan Sebagian	2

No	Pertanyaan	Status	Skor
2	Apakah instansi/perusahaan anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	Dalam Penerapan / Diterapkan Sebagian	2
3	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	2
4	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	2
5	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Dalam Penerapan / Diterapkan Sebagian	2
6	Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	2
7	Apakah semua pelaksana pengamanan informasi di instansi/perusahaan anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Dalam Penerapan / Diterapkan Sebagian	2
8	Apakah instansi/perusahaan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Dalam Penerapan / Diterapkan Sebagian	2
9	Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	4
10	Apakah instansi/perusahaan anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	Dalam Penerapan / Diterapkan Sebagian	4
11	Apakah instansi/perusahaan anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?	Dalam Penerapan / Diterapkan Sebagian	4
12	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasikan persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?	Dalam Penerapan / Diterapkan Sebagian	4
13	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?	Dalam Penerapan / Diterapkan Sebagian	4
14	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?	Dalam Penerapan / Diterapkan Sebagian	4
15	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan instansi/perusahaan secara rutin dan resmi?	Dalam Penerapan / Diterapkan Sebagian	4
16	Apakah kondisi dan permasalahan keamanan informasi di instansi/perusahaan anda menjadi konsiderans atau bagian dari proses pengambilan keputusan strategis di instansi/perusahaan anda?	Dalam Penerapan / Diterapkan Sebagian	4
17	Apakah pimpinan satuan kerja di instansi/perusahaan anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	Dalam Penerapan / Diterapkan Sebagian	6
18	Apakah instansi/perusahaan anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya,	Dalam Penerapan / Diterapkan Sebagian	6

No	Pertanyaan	Status	Skor
	pemantauannya dan eskalasi pelaporannya?		
19	Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksanannya?	Dalam Penerapan / Diterapkan Sebagian	6
20	Apakah instansi/perusahaan anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan instansi/perusahaan?	Dalam Penerapan / Diterapkan Sebagian	6
21	Apakah instansi/perusahaan anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	Dalam Penerapan / Diterapkan Sebagian	6
22	Apakah instansi/perusahaan anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Dalam Penerapan / Diterapkan Sebagian	6
		Total	**84**

Pertanyaan-pertanyaan pada Tabel 1 merupakan kriteria penilaian Indeks KAMI dengan kondisi yang dimiliki oleh Kota XYZ. Hasil dari penilaian ini menggambarkan mengenai hal yang dapat ditingkatkan atau kembangkan menjadi lebih baik.

3.2. Pengukuran Risiko dengan NIST SP 800-30

a. *Assets Identification*

Aset harus dilindungi serta dipelihara demi keberlangsungan operasional, keamanan, dan kesejahteraan para penduduk yang datanya tersimpan. Aset yang dilindungi dapat berupa perangkat keras maupun lunak. Dalam konteks bagian Tata Kelola, aset yang perlu dilindungi diantaranya kebijakan, data dan informasi, edukasi keamanan informasi, penanggung jawab, program yang dilaksanakan, aspek hukum, penerapan *business continuity plan* dan *disaster recovery plan*, standar keamanan informasi, dan kinerja pengelolaan keamanan informasi. Berbagai aset ini sudah tercantum secara lengkap pada Tabel 1.

b. *Threat Sources* dan *Threat Event*

Sumber ancaman dan kejadiannya dapat dilihat pada tabel yang menjelaskan *Threat Sources* dan *Threat Event*.

Tabel 2. Pendefinisian *Threat Sources* dan *Threat Event*

No	Aset	*Threat Sources*	*Threat Event*
1	Kebijakan	Karyawan atau Internal	a) Terjadinya pelanggaran atau kasus yang menganggu operasional atau keberlangsungan program b) Penjabaran atau pembagian kerja yang tidak sesuai sehingga program tidak berjalan atau direncanakan
2	Data dan Informasi	a) Karyawan atau Internal b) Pelaku Eksternal c) Bencana Alam	a) Kehilangan data karena *human error* b) Kehilangan data karena kerusakan *hardware* c) Kehilangan data karena serangan *malware* d) Kehilangan data karena *ransomware* e) Kebocoran data melalui *phishing* f) Kebocoran data melalui *insider threat* g) Kebocoran data melalui *misconfiguration* h) Manipulasi data pengguna atau *master* i) Pencurian data pribadi atau intelektual j) Pencurian data pribadi atau intelektual k) Penghancuran data secara sengaja l) Terjadinya bencana alam (kebakaran, banjir, dan sejenisnya)
3	Edukasi Keamanan Informasi	a) Karyawan atau Internal b) Pelaku Eksternal	a) Mengklik tautan *phishing* b) Membuka lampiran email yang mencurigakan c) Menginstal *software* dari sumber yang tidak terpercaya d) Mengungkapkan informasi sensitif di *media social* e) Menggunakan Wi-Fi publik tanpa VPN

No	Aset	*Threat Sources*	*Threat Event*
			f) Karyawan tidak mengetahui kinerja atau fungsi tata Kelola g) Mengklik tautan *phishing* h) Membuka lampiran email yang mencurigakan i) Menginstal *software* dari sumber yang tidak terpercaya j) Mengungkapkan informasi sensitif di *media social* k) Menggunakan Wi-Fi publik tanpa VPN
4	Penanggung Jawab	Karyawan atau Internal	a) Gagal melapor insiden keamanan b) Gagal memberikan training keamanan kepada karyawan c) Gagal menerapkan kontrol keamanan yang tepat d) Gagal melakukan *patching* dan *update software*
5	Program yang Dilaksanakan	a) Karyawan atau Internal b) Pelaku Eksternal	a) Gagal dalam melaksanakan kinerja dan program b) Tidak menerapkan atau merencanakan program yang mendukung kinerja
6	Aspek Hukum	a) Karyawan atau Internal b) Pelaku Eksternal	Ketidaksesuaian atau pelanggaran terhadap UU dan regulasi yang berlaku
7	Penerapan *Business Continuity Plan* (BCP) dan *Disaster Recovery Plan* (DRP)	a) Karyawan atau Internal b) Bencana Alam	a) Gagal melakukan backup data b) Gagal melakukan restore data c) Gagal memindahkan sistem ke penyimpanan cadangan d) Gagal berkomunikasi dengan *stakeholders*
8	Standar Keamanan Informasi	a) Karyawan atau Internal b) Pelaku Eksternal	Ketidakpatuhan terhadap kerangka kerja keamanan informasi seperti ISO dan NIST
9	Kinerja dan Pengelolaan Keamanan Informasi	a) Karyawan	b) Prosedur yang salah ketika terjadi serangan siber. c) Tidak adanya penanggung jawab ketika terjadi serangan siber.

c. *Vulnerabilities*

Berdasarkan ancaman yang telah ditentukan adapunkerentanan yang dapat dideskripsikan sebagai berikut.

Tabel 3. Pendefinisian *Vulnerabilities*

Aset	*Vulnerabilites*
Kebijakan	a) Tidak adanya kebijakan yang mendukung program pelaksanaan Tata Kelola b) Tidak adanya kebijakan yang mengukur dan terkait Tata Kelola yang telah berjalan
Data dan Informasi	a) Data disimpan secara tidak aman (misalnya, dalam file teks biasa atau tanpa enkripsi). b) Kontrol akses tidak memadai (misalnya, terlalu banyak orang yang memiliki akses ke data sensitif). c) Sistem tidak di-patch atau diperbarui secara berkala. d) *Backup* data tidak memadai.
Edukasi Keamanan Informasi	a) Kurangnya program edukasi keamanan untuk karyawan. b) Karyawan tidak mengetahui tentang risiko keamanan informasi. c) Karyawan tidak tahu cara melindungi diri dari ancaman *cyber*.
Penanggung Jawab	d) Kurangnya akuntabilitas untuk keamanan informasi. e) Karyawan tidak tahu siapa yang bertanggung jawab untuk keamanan informasi. f) Tidak ada proses untuk merespons insiden keamanan.
Program yang Dilaksanakan	a) Gagal dalam melaksanakan kinerja dan program b) Tidak menerapkan atau merencanakan program yang mendukung kinerja
Aspek Hukum	a) Organisasi tidak mematuhi peraturan terkait keamanan informasi seperti contohnya UU ITE. b) Organisasi tidak memiliki rencana untuk merespons pelanggaran data sesuai hukum yang berlaku.
Penerapan *Business Continuity Plan* (BCP) dan *Disaster Recovery Plan* (DRP)	a) *Business Continuity Plan* dan *Disaster Recovery Plan* (BCP/DRP) tidak memadai. b) BCP/DRP tidak diuji secara berkala. c) Karyawan tidak tahu cara melaksanakan BCP/DRP. d) Tidak adanya tenaga ahli IT.
Standar Keamanan Informasi	a) Organisasi tidak mematuhi standar keamanan informasi. b) Kontrol keamanan tidak memadai. c) Tidak adanya pedoman atau prosedur kerangka kerja keamanan informasi yang diikuti.

Aset	*Vulnerabilites*
	d) Sistem tidak di-*patch* atau diperbarui secara berkala.
Kinerja dan Pengelolaan Keamanan Informasi	a) Kurangnya visibilitas terhadap risiko keamanan b) Kurangnya proses untuk mengelola risiko keamanan c) Kurangnya sumber daya untuk mengelola keamanan informasi d) Kurangnya pelatihan untuk staf keamanan informasi

d. *Likelihood*

Adapun rentang atau seberapa sering terjadinya suatu peristiwa dikategorikan pada tabel berikut[8]:

Tabel 4. *Likelihood Levels*

Likelihood Levels	**Frekuensi terjadi dalam satu tahun**
Very Low	$X < 2$
Low	$2 \leq X \leq 5$
Moderate	$6 \leq X \leq 9$
High	$10 \leq X \leq 12$
Very High	$X > 12$

Selain itu, kelima *levels* tersebut juga dapat dikategorikan sebagai seberapa besar kerusakan yang dapat ditimbulkan. Adapun hasil *likelihood* yang didapatkan berdasarkan aspek-aspek yang telah ditentukan adalah sebagai berikut:

Tabel 5. Risiko dan Kemunginan Terjadi

No	**Risiko**	**Kemungkinan Peristiwa yang Terjadi**	**Menghasilkan Dampak Buruk**	**Keseluruhan Kemungkinan**
1	Perencanaan program yang tidak baik, mulai dari pengoperasian, manajemen, pembagian kerja dan sebagainya	*Low*	*High*	*Moderate*
2	Kehilangan, manipulasi, dan kebocoran Data	*Very High*	*Very High*	*Very High*
3	Kurangnya edukasi atau program yang mendukung keamanan informasi untuk karyawan atau sumber daya manusia	*Very Low*	*Moderate*	*Low*
4	Tidak adanya penanggung jawab ketika terjadi insiden dan sumber daya manusia yang kurang memadai	*Moderate*	*Moderate*	*High*
5	Pogram yang dijalankan tidak sesuai	*Low*	*High*	*Moderate*
6	Semua kebijakan yang dibangun atau dijalankan tidak sesuai dengan hukum yang berlaku	*Very Low*	*High*	*Moderate*
7	Penerapan atau respon terhadap insiden (aspek BCP/DRP) tidak dijalankan atau berjalan dengan baik	*Moderate*	*Very High*	*High*
8	Standar keamanan informasi yang tidak dijalankan dengan baik	*Very Low*	*Very High*	*Low*
9	Kinerja atau langkah yang dilakukan dalam menghadapi insiden tidak berjalan dengan baik	*Low*	*High*	*Moderate*

e. *Impact*

Berdasarkan risiko dari tiap aspek yang dijelaskan pada tabel 5, berikut penjelasan risiko dan kemungkinan terburuk yang dapat terjadi:

Tabel 6. Penjabaran Risiko

Risiko	**Keterangan**	**Dampak Maksimal**
Perencanaan program yang tidak baik, mulai dari pengoperasian, manajemen, pembagian kerja dan sebagainya	Dampak *High* karena memiliki dampak berantai, luas, merugikan dalam jangka panjang dan sulit untuk diperbaiki.	*High*
Kehilangan, manipulasi, dan kebocoran Data	Dampak *Very High* karena berpotensi untuk menghancurkan organisasi dengan dampak finansial yang besar, kerusakan reputasi, tuntunan hukum dan lain-lain.	*Very High*
Kurangnya edukasi atau program yang mendukung keamanan	Dampak *Moderate* karena memiliki dampak tidak langsung dan sudah terdapat mekanisme	*Moderate*

Risiko	Keterangan	Dampak Maksimal
informasi untuk karyawan atau sumber daya manusia	pengamanan, akan tetapi terkadang insiden besar juga dapat dikategorikan kesalahan karyawan.	
Tidak adanya penanggung jawab ketika terjadi insiden dan sumber daya manusia yang kurang memadai	Dampak *Moderate* karena tergamtung insiden yang dihadapi serta sudah terdapat mekanisme pengamanan atau prosedur.	*High*
Program yang dijalankan tidak sesuai	Dampak *High*, karena program yang tidak sesuai mengakibatkan adanya kerentanan.	*Very High*
Semua kebijakan yang dibangun atau dijalankan tidak sesuai dengan hukum yang berlaku	Dampak *High*, karena dibutuhkan suatu kebijakan yang mendukung keamanan sistem informasi, serta terdapat juga sanksi hukum yang berlaku.	*Very High*
Penerapan atau respon terhadap insiden (aspek BCP/DRP) tidak dijalankan atau berjalan dengan baik	Dampak *Very High*, karena BCP/DRP merupakan langkah pengamanan ketika terjadi insiden	*Very High*
Standar keamanan informasi yang tidak dijalankan dengan baik	Dampak *Very High*, karena standar keamanan menjamin suatu organisasi aman dan terhindar dari berbagai skenario buruk.	*Very High*
Kinerja atau langkah yang dilakukan dalam menghadapi insiden tidak berjalan dengan baik	Dampak *High* karena tidak adanya prosedur atau langkah mitigasi mengatasi insiden.	*Very High*

f. *Risk Determination*

Bertujuan untuk menentukan risiko mana yang memiliki kemungkinan atau peluang yang paling tinggi sehingga dapat dilakukan langkah prioritas. Berikut hasil *risk determination*:

Tabel 7. Penentuan Risiko

No	Risiko	Keseluruhan Kemungkinan	Dampak Maksimal	*Level Risk Determination*
1	Perencanaan program yang tidak baik, mulai dari pengoperasian, manajemen, pembagian kerja dan sebagainya	*Moderate*	*High*	*High*
2	Kehilangan, manipulasi, dan kebocoran Data	*Very High*	*Very High*	*Very High*
3	Kurangnya edukasi atau program yang mendukung keamanan informasi untuk karyawan atau sumber daya manusia	*Low*	*Moderate*	*Moderate*
4	Tidak adanya penanggung jawab ketika terjadi insiden dan sumber daya manusia yang kurang memadai	*High*	*High*	*High*
5	Pogram yang dijalankan tidak sesuai	*Moderate*	*Very High*	*High*
6	Semua kebijakan yang dibangun atau dijalankan tidak sesuai dengan hukum yang berlaku	*Moderate*	*Very High*	*High*
7	Penerapan atau respon terhadap insiden (aspek BCP/DRP) tidak dijalankan atau berjalan dengan baik	*High*	*Very High*	*High*
8	Standar keamanan informasi yang tidak dijalankan dengan baik	*Low*	*Very High*	*Moderate*
9	Kinerja atau langkah yang dilakukan dalam menghadapi insiden tidak berjalan dengan baik	*Moderate*	*Very High*	*High*

4. Kesimpulan

Hasil dari penelitian yang telah dilakukan berdasarkan hasil penilaian Indeks KAMI pada pemerintah XYZ, didapatkan jika terdapat aspek KAMI yang kurang baik dibandingkan aspek lainnya yaitu Tata Kelola. Bagian ini dijabarkan kembali dengan menggunakan penilaiain risiko dengan NIST 800-30 sehingga didapatkan level risiko serta ancaman yang mungkin terjadi, dengan demikian pemerintah XYZ dapat menanggulangi atau memperbaiki berbagai risiko atau ancaman yang telah dikaji demi meningkatkan kinerja serta keamanan. Selain itu, dapat juga lebih mendifinisikan mengenai ancaman lainnya dan mengkaji ulang ancaman tersebut sebagai prospek penelitian berikutnya.

Daftar Pustaka

[1] T. Rochmadi And I. Y. Pasa, "Measurement Of Risk And Evaluation Of Information Security Using The Information Security Index In Bkd Xyz Based On Iso 27001 / Sni," 2021.

[2] Chazar Chalifa, "Standar Manajemen Keamanan Sistem Informasi Berbasis Iso/Iec 27001:2005," 2015. [Online]. Available: Www.Republika.Co.Id.

[3] D. Setiya Budi And A. Tarigan, "Konsep Dan Strategi Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) Dan Evaluasi Kesadaran Keamanan Informasi Pada Pengguna," *Tahun*, Vol. 2, No. 1, 2018.

[4] A. Rizky, A. Setyawan, And M. Riza Akbar Pramudya," Penilaian Risiko Teknologi Informasi Dan Keamanan Informasi Menggunakan Framework Nist Sp 800-30 (Studi Kasus : E-Learning Universitas Pembangunan Nasional Veteran Jakarta)." 2021. [Online]. Available: Https://Elearning40.Upnvj.Ac.Id/.

[5] A. R. Riswaya, A. Sasongko, A. Maulana, S. Mardira Indonesia, And U. Langlangbuana Bandung, "Evaluasi Tata Kelola Keamanan Teknologi Informasi Menggunakan Indeks Kami Untuk Persiapan Standar Sni Iso/Iec 27001 (Studi Kasus: Stmik Mardira Indonesia)," *Jurnal Computech & Bisnis*, Vol. 14, No. 1, Pp. 10–18, 2020.

[6] L. D. A. Jelita, M. N. Al Azam, And A. Nugroho, "Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 Dan Iso/Eic 27001:2022," *Jurnal Saintekom*, Vol. 14, No. 1, Pp. 84–94, Mar. 2024, Doi: 10.33020/Saintekom.V14i1.623.

[7] R. Ramadhan Putra, E. Setiawan, And A. Ambarwati, "Analisis Manajemen Risiko Ti Pada Keamanan Data E-Learning Dan Aset Ti Menggunakan Nist Sp 800-30 Revisi 1," *Jurnal Teknik Informatika Dan Sistem Informasi*, Vol. 6, No. 1, 2019, [Online]. Available: Http://Jurnal.Mdp.Ac.Id.

[8] I. Gede, P. Krisna Juliharta, P. Anugrah, C. Dewi, And N. P. Widiari, "Analysis And Design Of Risk Management System Of Electronic Government (E-Government) (Study Case: Xyz Institutions)," P Issn, 2023.