The Indonesian Journal of Computer Science
www.ijcs.net
Volume 13, Issue 4, August 2024
https://doi.org/10.33022/ijcs.v13i4.4129

Manajemen Risiko Keamanan Informasi: Studi Kasus Pusat Data Dinas XYZ

Ramadhoni Putra[1], Setiyadi Yazid[2]
ramadhoni03@gmail.com[1], setiadi@cs.ui.ac.id[2]
[1,2] Universitas Indonesia

Informasi Artikel

Diterima : 13 Jun 2024
Direvisi : 25 Jun 2024
Disetujui : 25 Jul 2024

Kata Kunci

Manajemen Risiko, Keamanan Informasi, ISO27005, NIST SP 800-30, CIS CSC

Abstrak

Banyaknya kasus serangan siber di instansi pemerintah Indonesia, menuntut kepastian pengamanan untuk melindungi data krusial yang dimiliki. Tingginya ketergantungan terhadap pusat data dan dalam rangka menjaga kredibilitas instansi, dibutuhkan suatu perencanaan manajemen risiko keamanan informasi untuk menjamin kerahasiaan, integritas, dan ketersediaan layanan pusat data. Dalam menyusun perencanaan manajemen risiko keamanan informasi pusat data, penelitian dilakukan dengan menggunakan kerangka kerja ISO/IEC 27005:2018 sebagai kerangka kerja utama dalam proses manajemen risiko, NIST SP 800-30 Rev. 1 sebagai panduan pelaksanaan aktivitas penilaian risiko, dan CIS CSC sebagai acuan penentuan rekomendasi. Dari penilaian risiko, terdapat 47 risiko yang teridentifikasi. Dari 47 risiko terdapat 30 risiko yang perlu di lakukan penanganan sedangkan 17 risiko lagi dapat di terima oleh organisasi.

Keywords

Risk Management, Information Security, ISO 27005, NIST SP 800-30, CIS CSC

Abstract

The increasing number of cyber attacks on government institutions in Indonesia demands assurance of security to protect crucial data. Given the high dependence on data centers and in order to maintain the credibility of these institutions, a comprehensive information security risk management plan is required to ensure the confidentiality, integrity, and availability of data center services. In developing the information security risk management plan for data centers, this research utilizes the ISO/IEC 27005:2018 framework as the primary framework in the risk management process, NIST SP 800-30 Rev. 1 as a guide for conducting risk assessment activities, and CIS CSC as a reference for determining recommendations. From the risk assessment, 47 risks were identified. Out of these 47 risks, 30 require mitigation, while the remaining 17 can be accepted by the organization.

Attribution-ShareAlike 4.0 International License

A. Pendahuluan

Dalam mendukung pemerintahan, diperlukan teknologi informasi dalam penerapan nya. Dengan menggunakan teknologi informasi, pemerintahan akan lebih transparan. Akan tetapi dengan saat ini banyak terjadi insiden keamanan informasi. Insiden keamanan adalah situasi di mana kebijakan atau prosedur keamanan dapat diabaikan atau dilanggar, yang dapat menimbulkan risiko pada kerahasiaan, integritas, dan ketersediaan sistem informasi atau data. Insiden ini terjadi ketika ancaman memanfaatkan kelemahan atau kerentanan dalam sistem [1][2].

Sesuai laporan Monitoring Siber tahun 2022 terdapat 976.429.996 total trafik anomali pada tahun 2022 dan hingga agustus 2023. Dengan dua (2) anomali tertinggi yaitu MyloBot Botnet dan MiningPool Other Malware. Selain itu berdasarkan laporan BSSN web defacement menjadi serangan terbanyak sebesar 2.348 kasus dan pada sektor pemerintahan merupakan sektor yang paling banyak menerima serangan sebesar 885 kasus dengan sebaran waktu penyerangan terbanyak terjadi ketika hari kerja[Bssn]

Insiden yang memberikan dampak negatif pada organisasi dapat menimbulkan risiko keamanan informasi pada operasional. Risiko keamanan informasi adalah risiko yang timbul dari hilangnya kerahasiaan, integritas, atau ketersediaan sistem informasi atau data yang berpotensi merugikan misi, fungsi, citra, atau reputasi organisasi [2][3].

Setiap penyelenggara sistem elektronik harus menerapkan manajemen risiko melalui analisis risiko, perumusan mitigasi, dan penanggulangan risiko untuk melindungi infrastruktur informasi vital dari gangguan, ancaman, dan hambatan[4].

Risiko adalah kemungkinan terjadinya kerugian akibat ancaman yang mengekspos kerentanan. Risiko terkait dengan kombinasi ancaman, kerentanan, dan konsekuensi dalam hal penciptaan, pengumpulan, kepemilikan, penyimpanan, pengambilan, dan pengungkapan informasi[5].

Manajemen risiko adalah rangkaian kegiatan yang dimulai dari identifikasi, penilaian, dan pengendalian risiko agar organisasi dapat mengambil tindakan untuk mengurangi kerugian potensial yang disebabkan oleh risiko[1]. Melalui manajemen risiko, organisasi dapat mengidentifikasi, mengevaluasi, dan mengurangi risiko keamanan informasi yang mungkin timbul dengan demikian manajemen risiko keamanan informasi dapat membantu mengatasi insiden keamanan meskipun tidak mungkin untuk menghilangkan sepenuhnya risiko keamanan informasi. Untuk mengendalikan risiko, terdapat tiga aktivitas utama yang harus dilakukan dalam manajemen risiko, yaitu identifikasi, penilaian, dan pengendalian risiko[15].

ISO/IEC 27005:2018 merupakan sebuah standar yang dibuat oleh ISO *(The International Organization for Standardization*) dan IEC *(International Electrotechnical Commission),* yang berisi pedoman manajemen risiko keamanan informasi yang dirancang untuk membantu pelaksanaan proses keamanan informasi berdasarkan pendekatan manajemen risiko. Proses manajemen risiko keamanan informasi terdiri atas penetapan konteks *(context establishment)*, penilaian *(risk assessment),* penanganan *(risk treatment),* penerimaan *(risk*

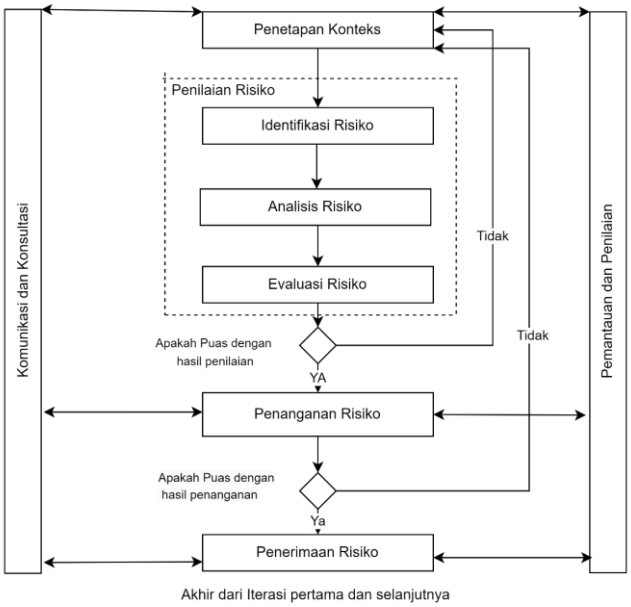
acceptance), komunikasi *(risk communication)* serta pemantauan dan peninjauan *(risk monitoring and review)* [6].

NIST SP 800-30 adalah sebuah standar yang diterbitkan oleh salah satu divisi di dalam *Department of Commerce* Amerika Serikat yang dikenal sebagai NIST. Standar ini berfungsi sebagai panduan untuk melakukan penilaian risiko terhadap sistem informasi yang digunakan oleh organisasi maupun pemerintahan. Penilaian risiko yang dijelaskan dalam standar ini merupakan sebuah proses yang bertujuan untuk mengidentifikasi, mengevaluasi, dan memberikan prioritas terhadap risiko yang muncul dari operasional sistem informasi[7].

Centre for internet security (CIS) *Critical Security Controls* (CSC), juga dikenal sebagai CIS Control, awalnya merupakan kegiatan sederhana yang bertujuan untuk mengidentifikasi serangan cyber yang paling umum dan signifikan yang mempengaruhi perusahaan sehari-hari. Setelah itu, pengetahuan dan pengalaman tersebut diubah menjadi tindakan positif dan konstruktif, yang kemudian dibagikan ke khalayak yang lebih luas untuk membantu orang dan perusahaan fokus pada langkah-langkah penting dalam mempertahankan diri dari serangan yang sangat penting[8].

B. Metode Penelitian

Penelitian ini dirancang untuk menyelesaikan masalah keamanan informasi pada pusat data dinas XYZ. Penilitian ini akan mengahasilkan rancangan keamanan informasi yang akan di gunakan dinas XYZ. Alur penelitian seperti gambar berikut:



Gambar 1. Alur Manajemen Risiko Keamanan Informasi

Pada penelitian ini terdapat tiga kerangka kerja yaitu ISO/IEC 27005, NIST SP 800-300 Rev. 1, dan CIS CSC. ISO/IEC 27005 dijadikan sebagai kerangka kerja utama dalam manajemen risiko keamanan informasi, karena sesuai dengan kebijakan yang telah ditetapkan oleh instansi pemerintah dalam penyelenggaraan SPBE. NIST SP 800-30 Rev.1 digunakan dalam salah satu aktivitas yang terdapat

dalam kegiatan manajemen risiko, yaitu penilaian risiko. Serta CIS CSC akan digunakan pada penanganan risiko.

1. Desain Penelitian

Penelitian ini menggunakan pendekatan kualitatif sebagai metode nya untuk membantu peneliti memahami fenomena manajemen risiko keamanan informasi di Dinas XYZ dalam konteks yang sesuai. Pendekatan kualitatif yang digunakan adalah studi kasus atau analisis mendalam suatu kasus, yaitu proses manajemen risiko keamanan informasi pada Pusat Data yang dimiliki oleh Dinas XYZ. Metode kualitatif dengan studi kasus ini didasarkan pada berbagai sumber data, seperti wawancara dengan narasumber, observasi, dan pengumpulan dokumen terkait penelitian. Penelitian studi kasus cocok untuk pertanyaan "bagaimana" dan "mengapa" [9].

Studi kasus merupakan metode penelitian yang cocok digunakan dalam kondisi khusus di mana terdapat banyak variabel yang mempengaruhi fenomena yang ingin dipelajari, sehingga diperlukan banyak sumber data yang berbeda untuk memastikan keakuratan hasil penelitian dengan melakukan triangulasi [10]. Studi kasus memanfaatkan beberapa metode pengumpulan data, seperti wawancara, observasi, pengumpulan dokumen, dan data sekunder

Tabel 1. Desain Penelitian

Elemen	Keterangan
Klasifikasi	Kualitatif
Kategori penelitian	Studi kasus
Tujuan penelitian	Membuat manajemen risiko keamanan informasi pada Pusat Data Dinas XYZ
Hasil penelitian	Manajemen risiko keamanan informasi pada Pusat Data Dinas XYZ
Pengumpulan data	Wawancara, observasi dan pengumpulan dokumen
Metode pemilihan narasumber	*Purposive sampling*
Metode pengolahan data	Analisis tematik

2. Metode Pengumpulan Data

Pendekatan penelitian kualitatif menggunakan berbagai jenis data, seperti teks, video, gambar, suara, dan tulisan, melalui berbagai metode pengumpulan data, daripada hanya mengandalkan satu sumber data [11]. Berikut ini adalah beberapa metode yang di lakukan untuk pengumpulan data pada penelitian ini.

a. Wawancara

Wawancara merupakan percakapan dengan tujuan yang dilakukan secara tatap muka atau melalui media telepon/konferensi secara *one-to-one* atau *one-to-many*[10]. Pengumpulan data melalui wawancara dilakukan terhadap narasumber pada dinas XYZ yang dipilih menggunakan teknik *purposive sampling*. Dengan teknik *purposive sampling* maka narasumber yang dipilih adalah yang dianggap memiliki pengetahuan dan kemampuan

terkait dengan topik penelitian. Narasumber dipilih sesuai dengan tugas dan tanggung jawabnya dalam organisasi yang terkait dengan pelaksanaan manajemen risiko, pengelolaan keamanan informasi, serta pelaksanaan pengembangan dan operasional pusat data. Data yang diperoleh dari wawancara menjadi data primer dari penelitian yang dilakukan.

b. Observasi

Observasi adalah metode penelitian di mana peneliti mencatat perilaku dan aktivitas objek penelitian secara langsung di lapangan. Peneliti dapat memiliki pertanyaan yang telah direncanakan sebelumnya atau tidak [11]. Observasi dilakukan dengan pengamatan pada dinas XYZ. Observasi dilakukan pada tahap pengumpulan data awal untuk menggali permasalahan mengenai penerapan manajemen risiko keamanan informasi dan tahap penilaian risiko dalam mengidentifikasi aset, ancaman, kerentanan, dampak, dan kontrol yang sudah diterapkan atas risiko.

c. Analisis dokumen

Pengumpulan dokumen dilakukan untuk mengumpulkan data pendukung terkait poin-poin pertanyaan wawancara. Dokumen yang di analisis merupakan dokumen formal dan informal meliputi kebijakan seperti rencana strategis organisasi, laporan kinerja organisasi, dan dokumen-dokumen seperti data riwayat serangan siber, laporan penilaian keamanan, dan lain-lain. Data yang diperoleh menjadi data sekunder dari penelitian yang dilakukan

3. Metode pengolahan data

Metode analisis tematik digunakan untuk mengolah data dalam penelitian ini. Analisis tematik melibatkan keterlibatan dan interpretasi yang lebih besar dari peneliti untuk mengidentifikasi dan menggambarkan ide yang tersurat maupun tersirat dalam data, yaitu tema. Untuk melakukan analisis ini, kode dikembangkan untuk mewakili tema yang teridentifikasi dan kemudian diterapkan pada data mentah sebagai penanda untuk analisis selanjutnya. Analisis tematik masih menjadi metode yang paling efektif dalam menangkap kompleksitas makna dalam kumpulan data teks[12].

Dalam analisis tematik, dilakukan proses coding terhadap transkrip wawancara untuk memberikan label pada data yang relevan dengan pertanyaan penelitian. Proses coding melibatkan penetapan label sebagai unit makna untuk potongan data yang dikumpulkan, sesuai dengan pendapat Recker [10]

4. Langkah pengumpulan data

Berikut langkah untuk tiap metode yang dilakukan:

a. Langkah pengumpulan data dengan metode wawancara semi terstruktur:
   i. Membuat kerangka pertanyaan umum. Wawancara yang dilakukan menggunakan wawancara deskriptif semi terstruktur yang membutuhkan kerangka pertanyaan menjaga alur wawancara tetap berjalan dalam jalur yang telah direncanakan. Wawancara yang

dilakukan berbentuk open ended questions untuk memperoleh jawaban yang lebih mendalam.

ii. Menentukan narasumber yang sesuai. Wawancara dilakukan terhadap koordinator, sub koordinator, dan staf yang berhubungan dengan kegiatan pengamanan SI/TI di lingkungan Dinas XYZ.

iii. Menyiapkan sarana wawancara, seperti buku catatan dan alat perekam.

iv. Melakukan wawancara yang dimulai dengan pertanyaan umum berdasarkan kerangka yang telah dirumuskan sebelumnya.

v. Menemukan hubungan antara topik dan isu yang diungkapkan narasumber yang berpotensi menjadi dasar untuk pertanyaan yang lebih spesifik yang tidak dirumuskan sebelumnya.

vi. Memberikan pertanyaan lanjutan untuk memperdalam isu yang diungkapkan narasumber

b. Langkah pengumpulan data dengan metode observasi:
   i. Mengamati kondisi aset-aset serta kontrol yang dimiliki pada pusat data.
   ii. Mencatat hasil pengamatan dalam lembar kerja.
c. Langkah pengumpulan data dengan metode pengumpulan dokumen:
   i. Mengidentifikasi kebutuhan dokumen.
   ii. Mengonfirmasi ketersediaan dokumen kepada Pejabat yang berwenang.
   iii. Meminta dokumen kepada staf yang bersangkutan.

5. Langkah pengolahan data

Berikut langkah yang dilakukan setelah proses pengumpulan data selesai:

a. Hasil wawancara di terjemah kan dalam bentuk transkrip (open coding). Open coding adalah proses identifikasi dan pemberian nama pada konsep-konsep dalam data yang dapat di kelompokkan ke dalam kategori yang lebih umum untuk mengurangi jumlah konsep yang tidak jelas atau tidak terungkap[13].
b. Dilakukan proses reduksi data, cleansing data, dan mengumpulkan data pokok yang diperlukan (open coding).
c. Membuat label-label penting terkait dan kodifikasi sesuai dengan kerangka kerja yang digunakan (axial coding), yaitu:
   i. Kode daftar aset.
   ii. Kode daftar ancaman.
   iii. Kode daftar kerentanan.
   iv. Kode kondisi predisposisi.
   v. Kode tipe dampak.

   Axial coding adalah proses mengategorikan data berdasarkan hubungan sebab-akibat untuk membedakan kondisi dari tindakan, interaksi, dan konsekuensi yang terjadi dalam data[14].
d. Meng analisa transkrip dengan memberikan label yang sesuai (axial coding).
e. Melakukan penilaian risiko berdasarkan hasil identifikasi.

f. Menentukan risiko yang harus di tindak lanjut.
g. Merancang penanganan risiko yang dapat terakomodasikan.
h. Hasil analisis data dan rekomendasi penanganan di validasi oleh organisasi.

Hasil dari proses analisis data pada tahap penetapan konteks adalah konteks manajemen risiko yang terdiri dari kriteria dasar, ruang lingkup, batasan, dan organisasi. Hasil dari proses analisis data pada tahap penilaian risiko adalah daftar hasil penilaian risiko.

C. Hasil dan Pembahasan

Terdapat beberapa hasil analisa dari penelitian ini, yaitu:

1. Penetapan Konteks

Kegiatan awal dalam melakukan manajemen risiko keamanan informasi dengan ISO 27005 dan juga sejalan dengan Permenpan RB No 5 Tahun 2020 adalah penetapan konteks. Dalam penetapan konteks dilakukan penetapan kriteria dasar, ruang lingkup, batasan, peran dan tanggung jawab pelaksana kegiatan manajemen risiko.

2. Identifikasi risiko

Pada tahap identifikasi terdapat beberapa hasil, yaitu:

a. Identifikasi aset

Aset adalah sesuatu yang bernilai bagi organisasi yang harus dijaga. Aset dapat berupa perangkat keras, perangkat lunak, data, informasi, personel, fungsi sistem, dan proses[1]. Kegiatan yang dilakukan adalah mengidentifikasi aset dalam organisasi yang berkaitan dengan operasional Pusat Data. Hasil identifikasi aset berpengaruh dalam penentuan dampak. Aset yang diidentifikasi pada Tabel 2 berikut adalah daftar aset yang telah diidentifikasi yang berlokasi di dinas XYZ.

Tabel 2. Indentifikasi aset

Kode	Jenis Aset	Nama Aset
A-1	Aset Pendukung	Aplikasi
A-2	Aset Pendukung	Server
A-3	Aset Pendukung	Fasilitas Pengamanan
A-4	Aset Pendukung	Perangkat Jaringan
A-5	Aset Pendukung	Personel
A-6	Aset Pendukung	Web Server
A-7	Aset Utama	Data

b. Identifikasi sumber ancaman

Kegiatan yang dilakukan adalah mengidentifikasi sumber ancaman yang harus diperhatikan. Untuk sumber ancaman adversarial, dilakukan penilaian kapabilitas, niat, dan karakteristik target. Sementara untuk sumber ancaman non adversarial, dilakukan penilaian rentang dampak.), Tabel 3 berikut adalah hasil identifikasi sumber ancaman adversarial.

Tabel 3. Sumber ancaman adversarial

Kode	Sumber Ancaman	Kapabilitas	Niat	Target
	Perorangan			
TA-1	o Pihak luar	5	4	5
TA-2	o Pihak dalam	1	1	1
	Organisasi			
TA-3	o Mitra	4	1	1
TA-4	o Negara	4	1	1

Pada tabel 4 berikut adalah hasil identifikasi sumber ancaman Non adversarial.

Tabel 4. Sumber ancaman Non adversarial

Kode	Sumber Ancaman	Rentang Dampak
	INSIDENTAL	
TB-1	- *User*	1
TB-2	- *Privileged User/Administrator*	4
	STRUKTURAL	
	- Perangkat TI	
TB-3	Perangkat Penyimpanan	4
TB-4	Perangkat Pemrosesan	3
TB-5	Perangkat Komunikasi & Keamanan	5
	- Perangkat Lunak	
TB-6	*Software*	2
TB-7	Sistem Operasi	2
TB-8	Jaringan	5
	LINGKUNGAN	
	- Bencana alam atau buatan	
TB-9	Api (Kebakaran/Ledakan)	5
TB-10	Gempa Bumi	5
	INSIDENTAL	
TB-11	Air (AC bocor/Saluran air bocor)	4
TB-12	Petir	4
TB-13	Pengerukan Tanah	4
	- Kegagalan/pemadaman infrastruktur	
TB-14	Kelistrikan	5

c. Identifikasi peristiwa ancaman

Organisasi mengidentifikasi bagaimana setiap peristiwa berpotensi membahayakan operasi organisasi, aset, individu, organisasi lain, atau bangsa. Relevansi yang dipilih memiliki hubungan langsung dengan toleransi risiko organisasi. Jika peristiwa ancaman dianggap tidak relevan, tidak ada pertimbangan lebih lanjut yang diberikan. Jika peristiwa ancaman dianggap relevan, organisasi mengidentifikasi semua sumber ancaman potensial yang

dapat memulai peristiwa tersebut. Untuk peristiwa ancaman yang telah dengan skala 5 (dikonfirmasi), organisasi telah mengonfirmasi bahwa peristiwa tersebut pernah terjadi di organisasi. Untuk peristiwa ancaman yang telah dengan skala 3 (diprediksi), peristiwa ancaman telah diprediksi organisasi berdasarkan kerentanan yang ada. Untuk peristiwa ancaman yang telah dengan skala 1 (mungkin). Pada tabel 5 merupakan hasil identifikasi peristiwa ancaman

Tabel 5. Identifikasi peristiwa ancaman

Kode	Peristiwa Ancaman	Sumber Ancaman	Relevansi
E-1	*Network sniffing*	TA-1	5
E-2	Serangan pada web (*phishing, web defacement, zero-day attack)*	TA-1	5
E-3	Serangan pada sistem yang tidak terkonfigurasi dengan baik (*exploit*, *malware)*	TA-1	5
E-4	Serangan DoS/DdoS	TA-1	5
E-5	*Unauthorized access*	TA-1	3
E-6	*Brute force login*	TA-1	3
E-7	*Man-in-the-middle attack*	TA-1	3
E-8	Pencurian data	TA-1; TA-2; TA-3	3
E-9	Memodifikasi/menghapus data	TA-1; TA-2; TA-3	3
E-10	Kebocoran informasi sensitif	TA-3; TB-1; TB-2	3
E-11	Kesalahan penanganan informasi penting	TB-2	1
E-12	Kesalahan pengaturan hak istimewa	TB-2	1
E-13	Kerusakan perangkat	TB-3; TB-4; TB-5 ; TB-14	5
E-14	Kegagalan fungsi sistem	TB-6	5
E-15	Paparan *vulnerabilities* ke dalam *software*	TB-6	5
E-16	Paparan *vulnerabilities* ke dalam sistem operasi	TB-7	3
E-17	Gangguan jaringan	TB-8	5
E-18	Kebakaran di area Pusat data	TB-9	1
E-19	Paparan air di area Pusat data	TB-11	5
E-20	Sambaran Petir	TB-12	5
E-21	Gempa di area Pusat data	TB-10	1
E-22	Kehilangan pasokan listrik	TB-12	5
E-23	Kabel FO Putus	TB-13	5
E-24	Gangguan penyedia telekomunikasi	TB-14	5

d. Identifikasi kontrol yang sudah ada

Kegiatan yang dilakukan adalah mengidentifikasi kontrol yang telah diterapkan pada masing-masing aset. Hasil identifikasi ini mempengaruhi

rekomendasi dalam penanganan risiko. Identifikasi kontrol dilakukan dengan cara melakukan penilaian berdasarkan kontrol yang dimiliki organisasi sesuai CIS CSC.

e. Perhitungan risiko

Kegiatan yang dilakukan melibatkan identifikasi risiko bagi organisasi dari peristiwa ancaman yang harus di utama kan, dengan mempertimbangkan seberapa mungkin peristiwa ancaman terjadi kemungkinan (Likelihood) dan dampak yang mungkin timbul (consequences). Sebelum melakukan evaluasi risiko, langkah awal adalah menilai kemungkinan dan tingkat dampaknya. Kemungkinan (Likelihood) ditetapkan berdasarkan seberapa sering peristiwa ancaman dapat terjadi dan seberapa besar dampak negatifnya, dengan mempertimbangkan sumber ancaman, kerentanan, dan faktor-faktor lain yang berkontribusi. Konsekuensi (consequences) ditetapkan dengan mempertimbangkan tingkat kerugian yang mungkin terjadi akibat peristiwa ancaman, juga dengan memperhatikan sumber ancaman, kerentanan, dan faktor-faktor kondisional lainnya. Pada tabel 6 merupakan hasil perhitungan risiko:

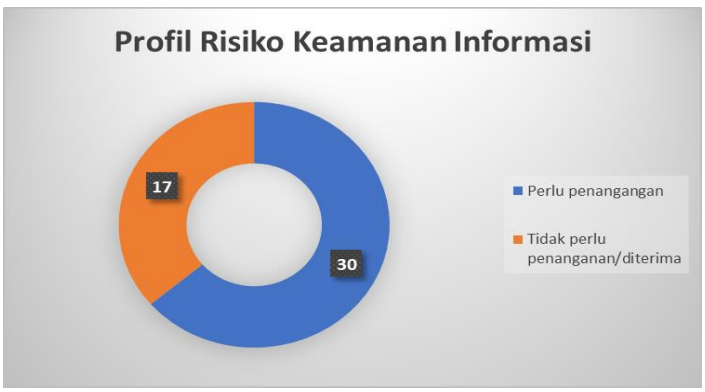
Tabel 6. Perhitungan risiko

Kode	Peristiwa Ancaman	*Likelihood*	Level Dampak	Risiko	Status Risiko	Penangaangan
RA-1	*Brute force login*	3	5	15	Sedang	Diperlukan
RA-2	Serangan DoS/DdoS	3	5	15	Sedang	Diperlukan
RA-3	Serangan pada sistem yang tidak terkonfigurasi dengan baik yang terpapar ke internet (exploit, malware)	3	5	15	Sedang	Diperlukan
RA-4	Serangan pada sistem yang tidak terkonfigurasi dengan baik yang terpapar ke internet (*exploit, malware)*	5	5	25	Sanggat Tinggi	Diperlukan
RA-5	*Unauthorized access*	3	5	15	Sedang	Diperlukan
RA-6	*Unauthorized access*	1	5	5	Sangat Rendah	Tidak Diperlukan
RA-7	Paparan *vulnerabilities* ke dalam sistem operasi	3	5	15	Sedang	Diperlukan
RA-8	Serangan pada web (*phishing, web* defacement*, zero-day attack)*	5	4	20	Tinggi	Diperlukan

RA-9	*Brute* force *login*	3	4	12	Sedang	Diperlukan
RA-10	*Unauthorized access*	3	4	12	Sedang	Diperlukan
RA-11	*Network sniffing*	3	4	12	Sedang	Diperlukan
RA-12	*Man-in-the-middle attack*	3	4	12	Sedang	Diperlukan
RA-13	*Unauthorized access*	3	4	12	Sedang	Diperlukan
RA-14	*Unauthorized access*	3	4	12	Sedang	Diperlukan
RA-15	*Unauthorized access*	1	4	4	Rendah	Tidak Diperlukan
RA-16	Pencurian data	3	5	15	Tinggi	Dimitigasi
RA-17	Pencurian data	1	5	5	Rendah	Tidak Diperlukan
RA-18	Memodifikasi/menghapus data	3	5	15	Tinggi	Diperlukan
RA-19	Memodifikasi/menghapus data	1	5	5	Rendah	Tidak Diperlukan
RA-20	Kebocoran informasi sensitif	3	5	15	Tinggi	Diperlukan
RB-1	Kesalahan pengaturan hak istimewa	3	3	9	Rendah	Tidak Diperlukan
RB-2	Kerusakan perangkat	3	4	12	Sedang	Diperlukan
RB-3	Paparan *vulnerabilities* ke dalam sistem operasi	5	3	15	Tinggi	Diperlukan
RB-4	Kebakaran di Pusat data	3	3	9	Rendah	Tidak Diperlukan
RB-5	Paparan Air di area Pusat data	3	3	9	Rendah	Tidak Diperlukan
RB-6	Sambaran Petir	5	3	15	Sedang	Diperlukan
RB-7	Gempa Di area Pusat Data	3	3	9	Rendah	Tidak Diperlukan
RB-8	Kehilangan pasokan listrik	5	3	15	Sedang	Diperlukan
RB-9	Kesalahan pengaturan hak istimewa	1	3	3	Rendah	Tidak Diperlukan
RB-10	Kegagalan fungsi sistem	5	3	15	Sedang	Diperlukan
RB-11	Kerusakan perangkat	5	3	15	Sedang	Diperlukan
RB-12	Gangguan Jaringan	5	3	15	Sedang	Diperlukan

RB-13	Kabel FO putus	5	5	15	Sedang	Diperlukan
RB-14	Kehilangan pasokan listrik	5	3	15	Sedang	Diperlukan
RB-15	Kebakaran di Pusat data	3	3	9	Rendah	Tidak Diperlukan
RB-16	Paparan air di area Pusdakim	3	3	9	Rendah	Tidak Diperlukan
RB-17	Gempa Bumi	3	3	9	Rendah	Tidak Diperlukan
RB-18	Sambaran Petir	5	3	15	Sedang	Diperlukan
RB-19	Kerusakan perangkat	5	3	15	Sedang	Diperlukan
RB-20	Kehilangan pasokan listrik	5	3	15	Sedang	Diperlukan
RB-21	Kebakaran di pusat data	3	3	9	Rendah	Tidak Diperlukan
RB-22	Kebakaran di pusat data	3	3	9	Rendah	Tidak Diperlukan
RB-23	Memodifikasi/menghapus data	3	2	6	Rendah	Tidak Diperlukan
RB-24	Kesalahan penanganan informasi penting	1	2	2	Rendah	Tidak Diperlukan
RB-25	Kesalahan pengaturan hak istimewa	1	2	2	Rendah	Tidak Diperlukan
RB-26	Paparan *vulnerabilities* ke dalam *software*	5	3	15	Sedang	Diperlukan
RB-27	Kesalahan penanganan informasi penting	3	5	15	Sedang	Diperlukan

Setelah melakukan perhitungan risiko maka di dapat profil keamanan informasi pada pusat data dinas XYZ sesuai gambar dibawah ini



Gambar 2. Profil keamanan informasi

f. Penanganan risiko

Setelah melakukan penilaian risiko dilakukan penanganan risiko dengan menggunakan CIS CSC. Terdapat 30 risiko yang akan di lakukan penanganan. Setiap risiko di lakukan analisa penanganan yang sesuai menurut CIS CSC version 7.

g. Penerimaan risiko

Setelah dilakukan penanganan risiko maka langkah terakhir di lakukan review oleh kepala dinas, berikut tabel 7 hasil rangkuman penerimaan risiko oleh organisasi.

Tabel 7. Penerimaan risiko

Kode	Risiko	Opsi Penanganan	Target Besaran Risiko
RA-1	15	Mengurangi kemungkinan	5 (Rendah)
RA-2	15	Mengurangi kemungkinan	5 (Rendah)
RA-3	15	Mengurangi kemungkinan serta dampak	3 (Rendah)
RA-4	25	Mengurangi dampak	10 (Rendah)
RA-5	15	Mengurangi kemungkinan	5 (Rendah)
RA-7	15	Mengurangi kemungkinan	5 (Rendah)
RA-8	20	Mengurangi dampak dan kemungkinan	9 (Rendah)
RA-9	12	Mengurangi kemungkinan	4 (Rendah)
RA-10	12	Mengurangi kemungkinan	4 (Rendah)
RA-11	20	Mengurangi kemungkinan serta dampak	9 (Rendah)
RA-12	12	Mengurangi dampak	9 (Rendah)
RA-13	12	Mengurangi kemungkinan	4 (Rendah)
RA-14	12	Mengurangi kemungkinan	4 (Rendah)
RA-16	15	Mengurangi kemungkinan	5 (Rendah)
RA-18	15	Mengurangi kemungkinan	5 (Rendah)
RA-20	15	Mengurangi kemungkinan	5 (Rendah)
RB-2	12	Mengurangi kemungkinan	4 (Rendah)
RB-3	15	Mengurangi kemungkinan	5 (Rendah)
RB-6	15	Mengurangi dampak	12 (Rendah)
RB-8	15	Mengurangi kemungkinan	5 (Rendah)
RB-10	15	Mengurangi dampak	9 (Rendah)
RB-11	15	Mengurangi kemungkinan	5 (Rendah)
RB-12	15	Mengurangi kemungkinan	5 (Rendah)
RB-13	15	Mengurangi dampak	5 (Rendah)
RB-14	15	Mengurangi kemungkinan	5 (Rendah)
RB-18	15	Mengurangi dampak	9 (Rendah)
RB-19	15	Mengurangi dampak	9 (Rendah)

RB-20	15	Mengurangi kemungkinan	5 (Rendah)
RB-26	15	Mengurangi kemungkinan	5 (Rendah)
RB-27	15	Mengurangi kemungkinan	5 (Rendah)

D. Simpulan dan Saran

Berdasarkan hasil penelitian yang telah dilakukan, manajemen risiko keamanan informasi yang dirancang untuk Pusat Data Dinas XYZ dibuat dengan cara penyusunan manajemen risiko keamanan informasi menggunakan kerangka kerja ISO/IEC 27005 sebagai kerangka kerja dasar untuk membentuk tahapan kegiatan manajemen risiko yaitu penetapan konteks, penilaian risiko, penanganan risiko dan penerimaan risiko. Penetapan konteks dilakukan berdasarkan NIST SP 800-30 dan PermenpanRB No. 5 Tahun 2020 dalam penyusunan kriteria sumber ancaman, relevansi peristiwa ancaman, tingkat kerentanan, kriteria kemungkinan, kriteria dampak, kriteria evaluasi, dan kriteria penerimaan risiko. NIST SP 800-30 sebagai kerangka kerja dalam pelaksanaan penilaian risiko, dan CIS CSC Version 7 sebagai kerangka kerja dalam penyusunan rancangan penanganan risiko. Penilaian risiko dilakukan dengan mengidentifikasi aset, sumber ancaman, peristiwa ancaman, kontrol eksisting pada aset, kerentanan perhitungan risiko. Dari perhitungan risiko, diidentifikasi 47 skenario risiko. Dari 47 risiko tersebut, 30 risiko perlu dilakukan penanganan sehingga harus dilanjutkan dengan rencana penanganan risiko. Sedangkan 17 risiko lainnya tidak perlu dilakukan penanganan. Penanganan risiko yang diusulkan dapat mengurangi kemungkinan insiden terjadi serta dampaknya. Setelah di lakukan review menggunakan opsi penanganan risiko tersebut, risiko tersebut dapat di terima organisasi

Saran

Keterbatasan dalam penelitian ini dapat dijadikan pengembangan pada penelitian berikutnya untuk mendapatkan rancangan manajemen risiko yang lebih komprehensif. Pada penanganan risiko dapat menerapkan dua atau lebih framework untuk mendapatkan hasil yang lebih baik. Perlu dilakukan analisis residual risk dan analisis biaya-manfaat dari penerapan kontrol pada tiap skenario risiko

E. Referensi

[1] Gibson, D., & Igonor, A. "*Managing Risk in Information Systems Third Edition. Jones & Bartlett Learning"*. 2022.

[2] NIST. "*NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments"*. NIST Special Publication. 2012

[3] Covert, E. (2023). "*Case Study: Conducting a Risk Assessment for an Electrical Utility"*. Proceedings of the 18th International Conference on Cyber Warfare and Security, 2023

[4] Peraturan Presiden Republik Indonesia. PP RI No 82 Tahun 2022 Tentang Perlindungan Infrastruktur Informasi Vital. 2022

[5] Saffady, W.Managing. "Information Risks: Threats, Vulnerabilities, and Responses". The Rowman & Littlefield. 2020

[6] ISO/IEC. "ISO/IEC 27005:2018 Information technology — Security techniques — Information security (Vol. 3, p. 56)". 2018

[7] NIST. “NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments”. NIST Special Publication, September. 2012
[8] CIS. “CIS Critical Security Controls, Version 7”.2021
[9] Yin, R. K. “Case Study Research and Applications: Design and Methods 6th Edition”. In *Journal of Hospitality & Tourism Research* (Vol. 53, Issue 5). Sage Publications, inc. 2018
[10] Recker, J. “Scientific Research in Information Systems: A Beginner’s Guide Second Edition”. Springer. 2021
[11] Creswell, J. W., & Creswell, J. D. “Research Design: Qualitative, Quantitative, and Mixed Methods Approaches Fifth Edition”. Sage Publications, Inc. 2018
[12] Guest, G., MacQueen, K. M., & Namey, E. E. “Applied Thematic Analysis”. Sage Publications. 2020
[13] Hennink, M., Hutter, I., & Bailey, A. “Qualitative Research Methods”. Sage Publications. 2020
[14] Saldaña, J. “The Coding Manual for Qualitative Researchers (4th ed.)”. Sage Publications]. 2021
[15] Whitman, M. E., & Mattord, H. J. “Principles of Information Security Sevent Edition. In Cengage Learning”. 2021