Journal of Applied Informatics and Computing (JAIC)
Vol.x, No.x, July 2026, pp. xxx~xxx
e-ISSN: 2548-6861

Analisis Risiko Keamanan Informasi Berbasis ISO/IEC 27001:2022 pada Pusat Kegiatan Belajar Masyarakat (PKBM) XYZ

Nabilah Fathimah [1]*, Antoni Haikal [2]**
* Rekayasa Keamanan Siber, Politeknik Negeri Batam
** Rekayasa Keamanan Siber, Politeknik Negeri Batam
nabilah.fathimah.hadi3@students.ac.id [1], antoni@polibatam.ac.id [2]

Article Info

Article history:

Received 17 July 2026
Revised 31 July 2026
Accepted ...

Keyword:

Information Security, Risk Analysis, Risk Assessment, ISO/IEC 27001:2022, PKBM.

ABSTRACT

PKBM XYZ utilizes various information technology assets to support its operational activities and educational services, including data, hardware, software, computer networks, and human resources. These resources face possible threats that could influence the confidentiality, integrity, and accessibility of data. Therefore, information security risk analysis is required as the basis for effective information security management. The aim of this research is to analyze the risks to information security at PKBM XYZ by utilizing the Risk Assessment approach aligned with the ISO/IEC 27001:2022 standard. The analysis was conducted through the identification of assets, threats, and vulnerabilities, followed by risk assessment and evaluation based on the likelihood of threats and their potential impact on the organization. Information was gathered via observations, interviews, and documentation to gain insights into the information technology resources and the present condition of information security related to this area of investigation. The results indicate that the administrator's laptop and router have the highest risk values, primarily due to inadequate physical protection and maintenance of hardware assets, while web hosting services and other network assets show relatively lower risk levels. Based on the risk evaluation results, information security control recommendations were developed in accordance with ISO/IEC 27001:2022 to support risk mitigation and enhance information security. The results from this research are anticipated to provide guidance for PKBM XYZ in enhancing its information security management in a more efficient manner.

I. PENDAHULUAN

Peningkatan teknologi informasi telah menunjang bermacam institusi pendidikan untuk memanfaatkan sistem serta infrastruktur digital dalam mendukung kegiatan operasional maupun proses pembelajaran. Pemanfaatan teknologi informasi memberikan berbagai manfaat, seperti meningkatkan efisiensi pengelolaan data, mempercepat proses pertukaran informasi, serta mendukung pengambilan keputusan yang lebih efektif. Namun, semakin tingginya ketergantungan terhadap teknologi informasi juga meningkatkan risiko terhadap keamanan aset informasi yang dimiliki organisasi [1].

Keamanan informasi menjadi salah satu dasar penting dalam mengawasi integritas (*integrity*), kerahasiaan (*confidentiality*), serta juga ketersediaan (*availability*) data. Gangguan terhadap salah satu aspek tersebut dapat menyebabkan berbagai kerugian bagi organisasi, seperti kehilangan data, gangguan operasional, akses tidak sah, hingga kerusakan sistem yang dapat memengaruhi kualitas layanan. Oleh karena itu, diperlukan upaya yang sistematis agar menandakan, menganalisis, serta manajemen risiko keamanan data agar aset yang dimiliki organisasi dapat terlindungi dari berbagai ancaman yang berpotensi terjadi.

PKBM (Pusat Kegiatan Belajar Masyarakat) XYZ termasuk lembaga pendidikan nonformal yang menyelenggarakan berbagai program pendidikan dan pelatihan bagi masyarakat. Dalam mendukung kegiatan operasional dan layanan pendidikan, PKBM XYZ memanfaatkan beberapa teknologi informasi, seperti perangkat keras, jaringan komputer, perangkat lunak, data akademik dan juga administrasi, serta sumber daya manusia yang terlibat dalam melakukan pengelolaan informasi. Aset-aset tersebut memiliki peran penting dalam mendukung keberlangsungan layanan organisasi sehingga memerlukan pengelolaan keamanan yang memadai.

Berdasarkan hasil observasi awal, terdapat beberapa potensi risiko yang dapat memengaruhi keamanan informasi di lingkungan PKBM XYZ, seperti kesalahan konfigurasi sistem, lemahnya pengelolaan hak akses, keterlambatan pembaruan perangkat lunak, kehilangan data akibat kegagalan perangkat, serta kemungkinan akses tidak sah terhadap sistem dan jaringan. Selain itu, meningkatnya penggunaan teknologi informasi juga membuka peluang munculnya berbagai ancaman siber yang dapat mengeksploitasi kerentanan pada aset teknologi informasi organisasi.

Usaha dalam meminimalkan dampak dari berbagai risiko tersebut diperlukan proses analisis risiko yang mampu mengidentifikasi aset sensitif, mengenali ancaman dan kerentanan yang berpotensi terjadi, serta menentukan tingkat risiko yang dihadapi organisasi. Hasil analisis risiko mampu dijadikan menjadi acuan landasan ketika menetapkan prioritas pengelolaan keamanan informasi dan juga menjadi pendukung dalam melakukan pengambilan keputusan yang lebih tepat dalam upaya perlindungan aset teknologi informasi.

ISO/IEC 27001:2022 termasuk dalam standar yang begitu sering dipakai pada pengelolaan keamanan informasi. Standar ini menyediakan kerangka kerja yang sistematis ketika menandakan, menganalisis, mengevaluasi, serta manajemen risiko keamanan data [2]. Melalui proses penilaian risiko yang mengacu pada standar tersebut, organisasi dapat memperoleh gambaran mengenai kondisi keamanan informasi yang dimiliki serta menentukan rekomendasi kontrol keamanan yang sesuai berdasarkan tingkat risiko yang ditemukan.

Berdasarkan uraian tersebut, kajian ini dilakukan agar menjalankan analisis risiko keamanan data di PKBM XYZ memakai metode *Risk Assessment* yang mengacu pada standar ISO/IEC 27001:2022. Pengumpulan data dilakukan melalui observasi, wawancara terhadap aset teknologi informasi yang menjadi objek kajian. Kajian ini dimaksudkan mampu membagikan wawasan terkait aset kritis, ancaman dan kerentanan yang dihadapi organisasi, tingkat risiko keamanan informasi, serta rekomendasi kontrol keamanan yang dapat digunakan sebagai acuan dalam meningkatkan keamanan informasi di lingkungan PKBM XYZ.

II. TINJAUAN PUSTAKA

A. Sistem Informasi

Sistem informasi termasuk suatu sistem yang merujuk berbagai komponen yang bekerja secara terintegrasi agar menghimpun, manajemen, menyimpan, serta membagikan wawasan guna menunjang aktivitas operasional serta kebutuhan organisasi [3]. Umumnya, sistem informasi mencakup bermacam komponen utama yang saling mendukung, yakni perangkat keras (*hardware*), perangkat lunak (*software*), data, prosedur, jaringan komunikasi (*network*), serta sumber daya manusia (*people*). Seluruh komponen tersebut bekerja secara terintegrasi untuk menghasilkan informasi yang akurat, relevan, dan tepat waktu sesuai kebutuhan organisasi. Sistem informasi di dunia pendidikan berperan penting dalam mendukung berbagai aktivitas akademik maupun administrasi. Pemanfaatan sistem informasi memungkinkan proses pengelolaan data peserta didik, administrasi pembelajaran, pengelolaan laboratorium, serta layanan akademik lainnya dapat dilakukan secara lebih cepat dan terstruktur. Selain itu, sistem informasi juga menjadi sarana pendukung dalam penyimpanan dan pertukaran informasi yang dibutuhkan oleh berbagai pihak dalam organisasi.

B. Keamanan Informasi

Keamanan informasi merupakan upaya agar mengawasi pemaparan dan aset pendukungnya dari bermacam ancaman yang dapat mengganggu kerahasiaan, integritas, serta adanya informasi [4]. Penerapan keamanan informasi bertujuan untuk menandakan yakni pemaparan hanya mampu terakses secara sah oleh pihak yang berwenang, tetap akurat, serta tersedia ketika dibutuhkan oleh pengguna yang sah. Organisasi bidang pendidikan nonformal mengadaptasi dunia digital akan menghadapi ancaman keamanan wawasan awalnya dari bermacam sumber, internal ataupun eksternal. Ancaman tersebut dapat berupa kerusakan perangkat keras, kegagalan sistem, serangan siber, akses tidak sah, kesalahan pengguna (*human error*), maupun penyalahgunaan hak akses yang berpotensi menimbulkan kerugian bagi organisasi.

Maka sebab itu, keamanan informasi jadi salah satu aspek krusial pada pengelolaan teknologi informasi karena berperan dalam menjaga keberlangsungan layanan, melindungi aset informasi, serta menunjang pencapaian tujuan organisasi secara efektif serta berkelanjutan.

C. CIA

CIA (*Confidentiality, Integrity, Availability*) merupakan prinsip landasan pada keamanan informasi yang dijalankan agar mengawasi serta melindungi aset informasi dari berbagai ancaman [5]. Ketiga aspek tersebut menjadi landasan dalam penerapan keamanan informasi karena digunakan untuk memastikan bahwa informasi tetap terlindungi, akurat, dan tersedia sesuai kebutuhan organisasi. Analisis risiko keamanan informasi pada prinsip CIA juga sering digunakan sebagai dasar dalam menentukan nilai dan tingkat kepentingan suatu aset informasi.

D. ISO/IEC 27001:2022

ISO/IEC 27001:2022 merupakan standar internasional yang digunakan sebagai pedoman pada manajemen keamanan data di suatu organisasi [6]. Standar ini mempermudah organisasi agar menjaga aset informasi melalui bermacam ancaman yang mampu menimbulkan kehilangan data, kerusakan sistem, ataupun gangguan layanan [7].

E. Kriteria Penilaian Risiko

1. Penilaian Risiko (*Risk Assessment*)

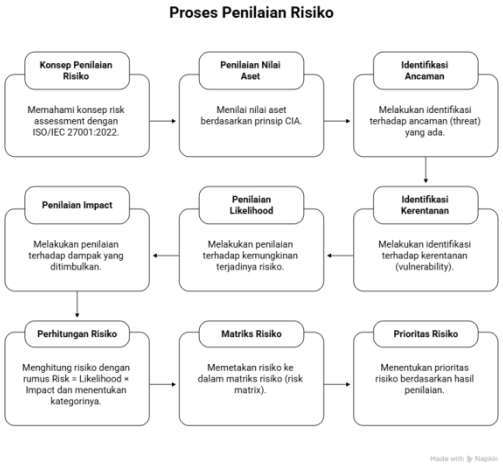
Penilaian risiko (*Risk Assessment*) termasuk pada aktivitas yang dilakukan agar menandakan, menganalisis, serta juga mengevaluasi risiko yang berpotensi memengaruhi aset organisasi [8]. Proses ini dilakukan dengan mengidentifikasi aset, ancaman, dan kerentanan yang ada, kemudian menentukan tingkat risiko melalui kemungkinan berlangsungnya ancaman (*Likelihood*) serta juga dampak yang bisa dihasilkan (*Impact*). Penilaian risiko dijalankan secara sistematis agar mendapat pemaparan terkait tingkat risiko yang dihadapi organisasi sehingga mampu dipakai menjadi dasar ketika menetapkan prioritas penanganan risiko [9]. Hasil penilaian risiko secara kualitatif membantu organisasi dalam memahami kondisi keamanan informasi serta menentukan rekomendasi kontrol yang sesuai untuk mengurangi risiko yang ditemukan. Dalam penelitian ini, tingkat risiko dihitung menggunakan pendekatan: *Risk = Likelihood × Impact*.

Nilai *likelihood* menunjukkan tingkat kemungkinan suatu ancaman dapat terjadi dengan mempertimbangkan kondisi keamanan dan kerentanan yang ditemukan pada objek penelitian. Dalam penelitian ini, nilai *Likelihood* diperoleh melalui konversi hasil wawancara berdasarkan instrumen penelitian yang disusun mengacu pada kontrol ISO/IEC 27001:2022. Konversi dilakukan menggunakan tabel konversi yang disusun oleh peneliti dengan prinsip bahwa semakin baik tingkat penerapan kontrol keamanan informasi berdasarkan hasil wawancara, maka semakin kecil kemungkinan (*Likelihood*) terjadinya risiko pada aset yang dianalisis. Pendekatan ini digunakan agar penilaian *Likelihood* dilakukan secara konsisten berdasarkan kondisi aktual yang diperoleh selama proses penelitian.

TABEL 1. *Likelihood*

Nilai Hasil Wawancara (Q)	Kondisi	Nilai *Likelihood*
5	Sangat Baik	1
4	Baik	2
3	Cukup	3
2	Kurang	4
1	Sangat Kurang	5

Sedangkan nilai *impact* menunjukkan tingkat dampak yang dapat ditimbulkan apabila risiko terjadi terhadap aset yang dinilai dengan mempertimbangkan tingkat kepentingan aset berdasarkan aspek *Confidentiality, Integrity,* dan *Availability* (CIA). Pendekatan ini digunakan untuk menjaga fokus penelitian pada analisis risiko keamanan data selaras pada ruang lingkup ISO/IEC 27001:2022.



Gambar 1. Proses Penilaian Risiko

2. Nilai Aset CIA

Penilaian ini dilakukan untuk mengetahui seberapa besar pengaruh aset terhadap keamanan informasi sehingga mampu dijalankan menjadi landasan pada proses analisis risiko. Metode yang dijalankan yakni pendekatan CIA (*Confidentiality, Integrity, Availability*) [10]. *Confidentiality* mengacu pada kemampuan untuk menjaga agar data hanya mampu diakses oleh pihak yang mempunyai hak akses. *Integrity* mengacu pada kemampuan untuk menjaga keakuratan, kelengkapan, dan keutuhan informasi agar tidak diubah secara tidak sah. Kemudian aspek *Availability* mengacu pada kemampuan untuk memastikan informasi dan

layanan mampu diakses oleh pihak yang berwenang saat diperlukan.

Nilai CIA digunakan menjadi dasar dalam menentukan tingkat dampak (*impact*) yang dapat terjadi apabila suatu aset mengalami gangguan keamanan. Dengan demikian, nilai aset tidak digunakan sebagai komponen perkalian langsung dalam perhitungan nilai risiko, tetapi digunakan untuk menggambarkan tingkat kepentingan aset dan menjadi salah satu dasar dalam menentukan impact. Penilaian konsisten terhadap setiap masing-masing aset aspek CIA diberikan skala nilai 1 - 5.

TABEL 2. Kriteria Penilaian Aset

Nilai	*Confidentiality* (Kerahasiaan)	*Integrity* (Integritas)	*Availability* (Ketersediaan)
1	Informasi bersifat umum dan tidak menimbulkan dampak apabila diketahui pihak lain.	Perubahan data tidak memberikan dampak yang berarti terhadap operasional.	Gangguan tidak memengaruhi operasional organisasi.
2	Informasi memiliki tingkat kerahasiaan rendah dan dampaknya kecil apabila bocor.	Perubahan data hanya memengaruhi sebagian kecil aktivitas.	Gangguan menyebabkan sedikit hambatan tetapi pekerjaan masih dapat berjalan.
3	Informasi memiliki tingkat kerahasiaan sedang dan memengaruhi sebagian proses operasional.	Perubahan data dapat mengganggu sebagian proses bisnis organisasi.	Gangguan menyebabkan beberapa layanan tidak berjalan sementara.
4	Informasi bersifat penting dan kebocorannya berdampak besar terhadap organisasi.	Perubahan data mengganggu operasional dan memerlukan pemulihan.	Gangguan menyebabkan sebagian besar layanan organisasi terhenti.
5	Informasi sangat rahasia dan kebocorannya dapat menyebabkan kerugian besar bagi organisasi.	Perubahan data menyebabkan kerusakan serius terhadap proses operasional.	Gangguan menyebabkan seluruh layanan utama organisasi tidak dapat digunakan.

Nilai aset diperoleh dengan menjumlahkan dari ketiga aspek tersebut. Semakin tinggi nilai aset yang diperoleh, maka semakin penting aset tersebut untuk dilindungi dan semakin besar dampak yang ditimbulkan dari berbagai ancaman dan kerentanan yang dapat mengganggu keamanan informasi. Perhitungan nilai aset dapat dilakukan memakai rumus yakni:

$$NA = NC + NI + NV$$

Keterangan:

NA = Nilai Aset (*Asset Value*), NC = Nilai *Confidentiality*, NI = Nilai *Integrity*, NV = Nilai *Availability*.

Hasil perhitungan nilai aset selanjutnya digunakan sebagai salah satu parameter dalam proses penilaian risiko keamanan informasi untuk menentukan tingkat risiko yang dimiliki oleh setiap aset [9].

3. Identifikasi Ancaman

Ancaman merupakan suatu kondisi atau kejadian yang berpotensi menimbulkan dampak terhadap aset informasi dan mengganggu aspek kerahasiaan (*confidentiality*), integritas (*integrity*), maupun ketersediaan (*availability*) informasi. Identifikasi ancaman dijalankan agar menentukan berbagai jenis ancaman yang berpeluang memengaruhi aset teknologi informasi pada PKBM XYZ. Penentuan jenis ancaman penelitian ini mengacu pada referensi yang relevan dengan keamanan informasi dan kemudian disesuaikan dengan karakteristik aset serta kondisi aktual pada objek penelitian. Kondisi aktual organisasi diperoleh melalui proses pengumpulan data menggunakan observasi dan kuesioner/wawancara.

Jenis ancaman yang dijalankan pada kajian ini ditata berdasar prinsip identifikasi ancaman pada proses manajemen risiko keamanan informasi mengacu pada ISO/IEC 27001:2022 [6], panduan NIST SP 800-30 Rev.1 *Guide for Conducting Risk Assessments* [8], serta didukung oleh literatur keamanan informasi yang membahas klasifikasi ancaman terhadap aset informasi [4], [5]. Daftar ancaman tersebut kemudian disesuaikan dengan kondisi aktual aset dan lingkungan operasional PKBM XYZ sehingga hanya ancaman yang relevan dengan objek penelitian yang digunakan dalam proses analisis risiko. Oleh sebab itu, ancaman yang digunakan dalam analisis risiko tidak hanya ditentukan berdasarkan asumsi peneliti, tetapi berdasarkan acuan referensi dan relevansinya terhadap lingkungan keamanan informasi pada PKBM XYZ.

TABEL 3. Daftar Ancaman

Kode	Jenis Ancaman	Acuan
T01	Akses tidak sah	[4], [5], [8]
T02	*Malware*	[4], [5]
T03	Kebocoran data	[5], [8], [11]
T04	Manipulasi data	[4], [5], [8]
T05	*Human error*	[5], [8]
T06	Gangguan layanan	[4], [8]
T07	Gangguan jaringan	[4], [8]
T08	Pencurian perangkat	[4], [5]
T09	Kerusakan perangkat	[4], [8]
T10	Listrik padam	[4], [8]
T11	*Phishing*	[4], [5]

4. Identifikasi Kerentanan

Kerentanan merupakan kelemahan atau kondisi pada aset, sistem, proses, maupun pengamanan yang dapat meningkatkan kemungkinan terjadinya suatu ancaman. Identifikasi kerentanan dilakukan berdasarkan kondisi aktual keamanan informasi pada PKBM XYZ yang didapat

pada wawancara, observasi, dan/atau kuesioner. Ancaman menunjukkan potensi kejadian yang dapat menyebabkan gangguan atau kerugian terhadap aset, sedangkan kerentanan menunjukkan kelemahan atau kondisi yang dapat memungkinkan atau meningkatkan kemungkinan terjadinya ancaman.

TABEL 4. Daftar Kerentanan

Kode	Kerentanan
V01	Pengelolaan informasi autentikasi pengguna belum optimal.
V02	Kurangnya pelatihan atau pemahaman pengguna dalam penggunaan sistem informasi.
V03	Pembaruan aplikasi dan perangkat lunak keamanan belum dilakukan secara berkala.
V04	Pengamanan fisik terhadap perangkat belum optimal.
V05	Pemeliharaan dan pemantauan kondisi perangkat belum dilakukan secara berkala.
V06	Pemeriksaan dan validasi data penting belum dilakukan secara berkala.
V07	Konfigurasi keamanan perangkat atau sistem belum ditinjau secara berkala.
V08	Pemeriksaan kondisi jaringan dan perangkat jaringan belum dilakukan secara berkala.
V09	Pengujian pemulihan data cadangan belum dilakukan secara berkala.
V10	Pengendalian akses terhadap sistem dan informasi belum optimal.

5. Klasifikasi Tingkat Risiko

Tingkat risiko dalam penelitian ini ditentukan berdasarkan hasil kombinasi antara nilai *Likelihood* dan *Impact.* Penilaian *Likelihood* mempertimbangkan kemungkinan terjadinya ancaman berdasarkan kondisi aktual keamanan informasi pada objek penelitian, sedangkan penilaian Impact mempertimbangkan tingkat kepentingan aset berdasarkan aspek *Confidentiality, Integrity,* dan *Availability* (CIA) serta konsekuensi yang dapat ditimbulkan terhadap aset apabila risiko terjadi. Hasil penilaian tersebut kemudian digunakan untuk mengklasifikasikan tingkat risiko dan menentukan prioritas penanganan risiko keamanan informasi melalui rekomendasi kontrol yang sesuai.

TABEL 5. Klasifikasi Tingkat Risiko

Rentang Nilai Risiko	Tingkat Risiko	Keterangan
12 – 18,4	*Very Low*	Risiko sangat rendah dan masih dapat diterima. Pemantauan dilakukan secara berkala.
18,4 – 24,8	*Low*	Risiko rendah, memerlukan pengendalian dasar agar tidak meningkat.
24,8 – 31,2	*Medium*	Risiko sedang, perlu dilakukan mitigasi sesuai prioritas organisasi.
31,2 – 37,6	*High*	Risiko tinggi, perlu segera diberikan pengendalian keamanan karena dapat memengaruhi operasional organisasi.
37,6 – 44	*Very High*	Risiko sangat tinggi, memerlukan tindakan pengendalian segera karena berpotensi mengganggu keberlangsungan layanan.

III. METODE

A. Metode Penelitian

Kajian ini memakai metode deskriptif melalui pendekatan kualitatif. Pendekatan kualitatif dijalankan agar memahami kondisi keamanan data yang terdapat pada PKBM XYZ melalui proses observasi, wawancara, serta identifikasi aset, ancaman, dan kerentanan yang dimiliki organisasi.

B. Tahapan Penelitian

Tahapan kajian dijalankan secara sistematis agar mendapat hasil analisis risiko keamanan informasi yang sesuai dengan tujuan kajian. Alur kajian akan nampak di Gambar 2.

1. Studi Literatur

   Tahap studi literatur dijalankan melalui mempelajari berbagai referensi yang berkaitan dengan keamanan informasi, manajemen risiko, penilaian risiko (*Risk Assessment*), serta standar ISO/IEC 27001:2022. Literatur diperoleh dari artikel kajian, jurnal ilmiah, serta dokumen penunjang lainnya yang kaitannya pada kajian.

2. Identifikasi Masalah

   Di tahap ini dijalankan identifikasi pada hambatan keamanan informasi yang ada di objek kajian berdasarkan hasil observasi dan studi literatur. Hasil identifikasi digunakan sebagai dasar dalam menentukan ruang lingkup penelitian.

3. Pengumpulan Data

   Penghimpunan data dijalankan berdasar observasi, dokumentasi, serta pengumpulan informasi terkait aset teknologi informasi yang dimiliki organisasi. Data yang dikumpulkan meliputi data aset, ancaman, kerentanan, serta informasi lain yang mendukung proses analisis risiko.

4. Identifikasi Aset

   Tahap identifikasi aset dilakukan agar menetapkan aset teknologi informasi yang menjadi objek analisis risiko. Aset yang diidentifikasi dapat berupa data, perangkat keras, perangkat lunak, jaringan komputer, maupun sumber daya manusia yang memiliki peran dalam pengelolaan informasi.

5. Analisis Risiko

   Analisis risiko dilakukan dengan mengidentifikasi ancaman yang relevan terhadap setiap aset berdasarkan acuan referensi yang digunakan, kemudian mengidentifikasi kondisi langsung dan kelemahan keamanan yang dapat memengaruhi kemungkinan

terjadinya ancaman. Selanjutnya, dilakukan penilaian *Likelihood* berdasarkan kemungkinan terjadinya ancaman dengan mempertimbangkan kondisi aktual keamanan informasi pada objek penelitian. Penilaian *Impact* ditentukan dengan mempertimbangkan tingkat kepentingan aset berdasarkan aspek *Confidentiality, Integrity,* dan *Availability* (CIA) serta konsekuensi yang dapat ditimbulkan apabila risiko terjadi. Hasil penilaian *Likelihood* dan *Impact* kemudian digunakan untuk menentukan tingkat risiko sebagai dasar dalam menetapkan prioritas penanganan dan rekomendasi kontrol keamanan data yang selaras pada ISO/IEC 27001:2022.

6. Penyusunan Laporan
   Tahap akhir pada penataan kajian melalui model laporan tugas akhir yang memuat hasil identifikasi aset, analisis risiko, evaluasi risiko, serta rekomendasi kontrol keamanan yang diusulkan.

Gambar 2. Tahapan Penelitian

C. Teknik Pengumpulan Data

Seluruh data dikumpulkan melalui metode teknis seperti berikut:

1. Observasi
   Metode observasi dijalankan melalui cara memantau secara langsung kondisi lingkungan PKBM XYZ yang berkaitan dengan pengelolaan teknologi informasi dan keamanan informasi. Observasi bertujuan untuk mengidentifikasi aset teknologi informasi yang digunakan dan mengetahui kondisi pengelolaan aset.

2. Wawancara
   Mengajukan pertanyaan kepada pihak yang bertanggung jawab terhadap pengelolaan teknologi informasi maupun aset informasi di PKBM XYZ. Tahapan ini bertujuan untuk memperoleh informasi mengenai proses operasional, pengelolaan aset, permasalahan keamanan informasi yang pernah terjadi, serta upaya pengamanan yang telah diterapkan oleh organisasi.

D. Teknik Analisis Data

Analisis data dijalankan memakai teknik analisis data kualitatif interaktif menurut Miles, Huberman, dan Saldaña (2020) [12]. Teknik ini dipilih karena menggunakan pengolahan data hasil observasi, wawancara, serta dokumentasi secara sistematis sehingga menghasilkan temuan yang dapat digunakan sebagai dasar dalam analisis risiko keamanan data berbasis ISO/IEC 27001:2022. Proses analisis data meliputi tiga tahapan dibawah.

1. Reduksi Data
   Data yang didapat pada observasi, wawancara, serta dokumentasi diseleksi, dirangkum, serta focus pada data yang berkaitan pada identifikasi aset, ancaman, kerentanan, dan kondisi keamanan informasi di PKBM XYZ.
2. Penyajian Data
   Data yang telah direduksi disusun melalui model tabel identifikasi aset, tabel ancaman, tabel kerentanan, matriks penilaian *Likelihood* dan *Impact*, serta matriks tingkat risiko agar memudahkan proses analisis dan interpretasi hasil penelitian.
3. Penarikan Kesimpulan
   Tahap ini dilakukan dengan menginterpretasikan hasil analisis risiko berdasarkan tingkat risiko yang diperoleh serta menyusun rekomendasi kontrol keamanan informasi yang mengacu pada ISO/IEC 27001:2022 Annex A sebagai upaya mitigasi risiko di PKBM XYZ.

E. Instrumen Penelitian

Pada kajian ini, instrumen yang dijalankan mencakup lembar observasi, pedoman wawancara atau kuesioner, serta formulir penilaian risiko. Lembar observasi dan pedoman wawancara atau kuesioner digunakan untuk memperoleh informasi mengenai aset, ancaman, kerentanan, serta kondisi aktual keamanan informasi pada PKBM XYZ. Selanjutnya, formulir penilaian risiko digunakan untuk mendokumentasikan hasil identifikasi dan penilaian risiko terhadap setiap aset berdasarkan kriteria penilaian yang telah dijalankan. Penghimpunan data dijalankan melalui tanya jawab beserta pemilik PKBM XYZ sebagai narasumber utama serta observasi secara langsung terhadap kondisi keamanan informasi pada objek penelitian. Berdasarkan hasil wawancara dan observasi tersebut, peneliti memberikan skor penilaian pada setiap indikator sesuai dengan kriteria yang digunakan dalam penelitian.

TABEL 6. Instrumen Kuesioner Penilaian Kondisi Keamanan Informasi

Kode	Aspek	Pertanyaan/Pernyataan	Acuan ISO/IEC 27001:2022
Q1	Kebijakan keamanan informasi	PKBM XYZ telah memiliki kebijakan atau aturan yang mengatur keamanan informasi yang digunakan dan dikelola oleh organisasi.	Annex A 5.1 – *Policies for information security*
Q2	Peran serta tanggung jawab keamanan informasi	Peran dan tanggung jawab pihak yang mengelola sistem informasi dan keamanan informasi telah ditetapkan dengan jelas.	Annex A 5.2 – *Information security roles and responsibilities*
Q3	Penggunaan aset informasi	Terdapat aturan mengenai penggunaan aset informasi dan aset TI yang digunakan dalam kegiatan PKBM XYZ.	Annex A 5.10 – *Acceptable use of information and other associated assets*
Q4	Pengendalian akses	Akses terhadap sistem informasi dan informasi diberikan sesuai dengan kebutuhan dan kewenangan pengguna.	Annex A 5.15 – *Access control*
Q5	Pengelolaan hak akses	Hak akses pengguna terhadap sistem informasi ditinjau dan diperbarui apabila terjadi perubahan kebutuhan atau kewenangan.	Annex A 5.18 – *Access rights*
Q6	Keamanan informasi dalam penggunaan layanan cloud	Penggunaan layanan web hosting atau layanan cloud yang mendukung sistem informasi dikelola dengan mempertimbangkan aspek keamanan informasi.	Annex A 5.23 – *Information security for use of cloud services*
Q7	Kesadaran dan pelatihan keamanan informasi	Pengelola dan pengguna sistem informasi telah memperoleh edukasi atau pelatihan mengenai keamanan informasi sesuai dengan perannya.	Annex A 6.3 – *Information security awareness, education and training*
Q8	Pelaporan kejadian keamanan informasi	Pengelola dan pengguna mengetahui cara melaporkan kejadian atau dugaan insiden keamanan informasi yang terjadi.	Annex A 6.8 – *Information security event reporting*
Q9	Keamanan fisik perangkat	Perangkat TI yang digunakan untuk mendukung sistem informasi dilindungi dari akses fisik yang tidak berwenang.	Annex A 7.2 – *Physical entry*
Q10	Perlindungan perangkat dari ancaman lingkungan	Perangkat TI dilindungi dari risiko lingkungan seperti gangguan suhu, listrik, dan kondisi lingkungan lain yang dapat mengganggu operasional perangkat.	Annex A 7.5 – *Protecting against physical and environmental threats*
Q11	Pemeliharaan perangkat	Perangkat TI dipelihara secara berkala untuk menjaga ketersediaan dan keamanan perangkat.	Annex A 7.13 – *Equipment maintenance*
Q12	Pengelolaan kerentanan teknis	Kerentanan teknis pada sistem dan perangkat *endpoint* diidentifikasi dan ditangani secara berkala.	Annex A 8.8 – *Management of technical vulnerabilities*
Q13	Perlindungan terhadap *malware*	Perangkat *endpoint* yang digunakan untuk mengakses atau mengelola informasi telah memiliki perlindungan terhadap *malware* dan dilakukan pemeriksaan atau pembaruan secara berkala.	Annex A 8.7 – *Protection against malware*
Q14	Pencadangan informasi	Informasi penting pada sistem informasi dicadangkan secara berkala melalui mekanisme pencadangan yang dapat digunakan untuk pemulihan apabila terjadi kehilangan atau kerusakan data.	Annex A 8.13 – *Information backup*
Q15	*Logging* dan *monitoring*	Aktivitas dan kejadian yang relevan dengan keamanan sistem dan perangkat TI dipantau serta ditinjau secara berkala.	Annex A 8.15 – *Logging; Annex A 8.16 – Monitoring activities*

IV. HASIL DAN PEMBAHASAN

Penghimpunan data pada kajian ini dijalankan melalui observasi, serta wawancara di PKBM XYZ. Berdasarkan proses tersebut diperoleh informasi mengenai aset teknologi informasi, kondisi pengelolaan keamanan informasi, potensi ancaman, serta dokumen pendukung yang digunakan sebagai dasar dalam proses analisis risiko keamanan informasi. Narasumber menjelaskan bahwa beberapa risiko yang berpotensi terjadi meliputi *human error*, lemahnya pengelolaan hak akses, kehilangan data akibat kerusakan perangkat, serta kemungkinan terjadinya akses tidak sah terhadap sistem informasi.

A. Hasil Identifikasi Aset

Berbagai kelemahan yang terdapat pada aset teknologi dapat diketahui dengan melakukan identifikasi kerentanan pada aset yang berpotensi dimanfaatkan sebagai ancaman sehingga dapat mengganggu keamanan maupun operasional sistem informasi. Kerentanan pada setiap aset diidentifikasi berdasarkan hasil observasi serta wawancara yang telah dijalankan. Hasil identifikasi tersebut akan nampak pada tabel dibawah.

TABEL 7. Daftar Aset TI PKBM

Kategori Aset TI	Nama Aset TI PKBM
Data	Data (sekolah, transaksi, nilai, peserta didik, mentor, dan pengelola)
Perangkat Lunak	Aplikasi sistem informasi akademik
Perangkat Keras	PC, router, modem, printer, dan laptop admin
Jaringan	LAN dan layanan web *hosting* (Hostinger)
Sumber Daya Manusia	Pengelola dan pengguna sistem informasi
Sarana Pendukung	AC

B. Hasil Nilai Aset CIA

Berdasarkan hasil identifikasi aset, setiap aset selanjutnya dilakukan penilaian menggunakan tiga aspek utama keamanan informasi (*Confidentiality, Integrity, and Availability*). Penilaian ini bertujuan untuk mengetahui

tingkat kepentingan setiap aset sehingga dapat digunakan sebagai dasar dalam proses analisis risiko keamanan data.

TABEL 8. Nilai Aset CIA

No.	Nama Aset	C	I	A	Nilai Aset
1.	Data (sekolah, transaksi, nilai, peserta didik, mentor, dan pengelola)	4	4	3	11
2.	Sistem informasi akademik	4	3	2	9
3.	Layanan web *hosting* (Hostinger)	4	4	4	12
4.	PC	2	3	3	8
5.	Router	3	3	4	10
6.	Modem	2	2	2	6
7.	Printer	1	2	2	5
8.	Laptop admin	4	4	3	11
9.	LAN	1	2	2	5
10.	Pengelola sistem informasi	4	3	3	10
11.	Pengguna sistem informasi	4	3	3	10
12.	AC	1	1	1	3

C. Hasil Identifikasi Ancaman dan Kerentanan Risiko

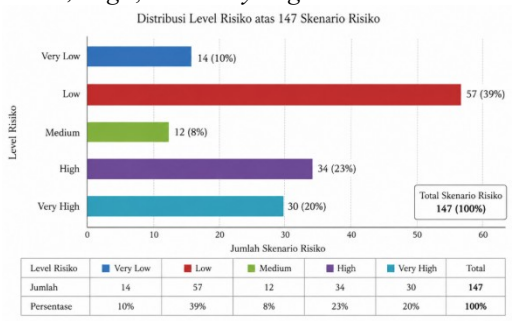
Berikut hasil identifikasi ancaman serta kerentanan Risiko yang mungkin dapat membahayakan sistem.

TABEL 9. Hasil Identifikasi Ancaman dan Kerentanan

Kategori Aset	Nama Aset	Kode *Threat*	Kode *Vulnerability*
Data	Data (sekolah, transaksi, nilai, peserta didik, mentor, dan pengelola)	T01, T02, T03, T04, T05.	V01, V06, V09.
Perangkat Lunak	Aplikasi Sistem Informasi Akademik	T01, T02, T04, T05, T06, T07.	V03, V05, V07
Jaringan	Layanan web *hosting* (Hostinger)	T01, T02, T03, T06.	V09.
Perangkat Keras	PC	T01, T02, T05, T08, T09, T10.	V01, V03, V04, V05.
Perangkat Keras	Router	T01, T06, T07, T09, T10.	V04, V05, V08.
Perangkat Keras	Modem	T01, T06, T07, T09, T10.	V04, V05, V08.
Perangkat Keras	Printer	T01, T05, T08, T09, T10	V04, V05.
Perangkat Keras	Laptop Admin	T01, T02, T05, T08, T09, T10.	V03, V04, V05.
Sarana Pendukung	AC	T09, T10.	V05.
Jaringan	LAN	T01, T06, T07, T09.	V05,V08.
Sumber Daya Manusia	Pengelola Sistem Informasi	T01, T05, T11.	V02.
Sumber Daya Manusia	Pengguna Sistem Informasi	T01, T05, T11.	V01, V02.

D. Hasil Nilai Risiko

Perhitungan nilai risiko dilakukan terhadap 147 skenario risiko yang merupakan kombinasi antara aset, ancaman, dan kerentanan berdasarkan hasil pemetaan sebelumnya. Nilai *Likelihood* diperoleh dari rata-rata hasil wawancara (Q) yang sesuai dengan setiap kerentanan, sedangkan nilai *Impact* menggunakan nilai aset yang diperoleh dari penilaian *Confidentiality, Integrity*, dan *Availability* (CIA). Selanjutnya, nilai risiko dihitung menggunakan rumus *Likelihood* × *Impact*. Beberapa skenario risiko yang memiliki kerentanan yang sama dapat menghasilkan nilai risiko yang sama meskipun ancaman yang dihadapi berbeda. Hal ini selaras pada metode kajian yang dijalankan di mana ancaman hanya berfungsi sebagai identifikasi jenis ancaman dan tidak diberi nilai numerik. Berdasarkan hasil perhitungan, nilai risiko berada pada rentang 12 hingga 44. Selanjutnya, level risiko ditentukan dengan membagi rentang nilai tersebut jadi lima kategori, yaitu *Very Low, Low, Medium, High*, serta *Very High*.



Gambar 3. Hasil Distribusi Nilai Risiko

Peringkat	Nama Aset	Risiko Tertinggi	Level Risiko
1	Laptop Admin	44	Very High
2	Router	40	Very High
3	Aplikasi Sistem	36	High
4	Data (sekolah, transaksi, nilai, peserta	33	High
5	PC	32	High
6	Pengguna Sistem	30	Medium
7	Pengelola Sistem	30	Medium
8	Modem	24	Low
9	Layanan Web Hosting	24	Low
10	LAN	20	Low
11	Printer	20	Low
12	AC	12	Very Low

Gambar 4. Rekap Prioritas Risiko

E. Evaluasi Risiko

Berdasarkan gambar 4 yang ditampilkan salah satunya aset Laptop Admin dan Router memiliki level risiko *Very High*. Tingginya risiko pada kedua aset tersebut dipengaruhi oleh kerentanan pada pengamanan fisik perangkat (V04), pemeliharaan perangkat yang belum dilakukan secara berkala (V05), serta pada Router juga dipengaruhi oleh pemeriksaan kondisi jaringan yang belum dilakukan secara berkala (V08). Oleh karena itu, kontrol yang direkomendasikan mengacu pada Annex A.7.8 *Equipment Siting and Protection*, A.7.13 *Equipment Maintenance*, dan A.8.20 *Networks Security*.

Aset Aplikasi Sistem Informasi Akademik, Data, dan PC berada pada level risiko *High*. Kerentanan utama pada aset tersebut meliputi pemeliharaan sistem yang belum optimal (V05), validasi dan perlindungan data (V06 dan V09), serta pengamanan fisik perangkat (V04). Rekomendasi kontrol mengacu pada Annex A.7.13 *Equipment Maintenance*, A.8.13 *Information Backup*, dan A.5.33 *Protection of Records*. Aset Pengelola dan Pengguna Sistem Informasi berada pada level risiko *Medium* karena masih terdapat kerentanan berupa kurangnya pelatihan dan pemahaman pengguna terhadap keamanan informasi (V02). Oleh karena itu, kontrol yang direkomendasikan adalah Annex A.6.3 *Information Security Awareness, Education and Training*.

Kemudian pada aset Layanan *web hosting*, Modem, Printer, dan LAN berada pada level risiko *Low*, sedangkan aset AC berada pada level *Very Low*. Meskipun tingkat risikonya relatif rendah, pengendalian keamanan tetap perlu dilakukan secara berkelanjutan untuk menjaga kondisi keamanan aset.

F. Penentuan Kontrol Keamanan

Penentuan Kontrol Keamanan dilakukan berdasarkan hasil analisis risiko pada setiap aset. Rekomendasi kontrol disusun dengan mengacu pada ISO/IEC 27001:2022 Annex A dan diselaraskan pada tingkat risiko yang diperoleh sebagai upaya mitigasi risiko keamanan informasi pada PKBM XYZ.

RINGKASAN: KERENTANAN, ANCAMAN & KONTROL ANNEX A – PER ASET (URUT PRIORITAS RISIKO)

No	Aset	Kerentanan (Vulnerability) Pemicu	Ancaman (Threat) Terkait	Risk Score	Level Risiko	Kontrol Annex A ISO/IEC 27001:2022
1	Laptop Admin	V04 - Pengamanan fisik terhadap perangkat belum optimal. V05 - Pemeliharaan dan pemantauan kondisi perangkat belum dilakukan secara berkala.	T01 (Akses tidak sah), T02 (Malware), T05 (Human error), T08 (Pencurian perangkat), T09 (Kerusakan perangkat), T10 (Listrik padam)	44	Very High	A.7.13 Equipment Maintenance A.7.8 Equipment Siting and Protection
2	Router	V04 - Pengamanan fisik terhadap perangkat belum optimal. V05 - Pemeliharaan dan pemantauan kondisi perangkat belum dilakukan secara berkala. V08 - Pemeriksaan kondisi jaringan dan perangkat jaringan belum dilakukan secara berkala.	T01 (Akses tidak sah), T06 (Gangguan layanan), T07 (Gangguan jaringan), T09 (Kerusakan perangkat), T10 (Listrik padam)	40	Very High	A.7.13 Equipment Maintenance A.7.8 Equipment Siting and Protection A.8.20 Networks Security
3	Aplikasi Sistem Informasi Akademik	V05 - Pemeliharaan dan pemantauan kondisi perangkat belum dilakukan secara berkala.	T01 (Akses tidak sah), T02 (Malware), T04 (Manipulasi data), T05 (Human error), T06 (Gangguan layanan), T07 (Gangguan jaringan)	36	High	A.7.13 Equipment Maintenance
4	Data (sekolah, transaksi, nilai, peserta didik, mentor, dan pengelola)	V06 - Pemeriksaan dan validasi data penting belum dilakukan secara berkala. V09 - Pengujian pemulihan data cadangan belum dilakukan secara berkala.	T01 (Akses tidak sah), T02 (Malware), T03 (Kebocoran data), T04 (Manipulasi data), T05 (Human error)	33	High	A.5.33 Protection of Records A.8.13 Information Backup
5	PC	V04 - Pengamanan fisik terhadap perangkat belum optimal. V05 - Pemeliharaan dan pemantauan kondisi perangkat belum dilakukan secara berkala.	T01 (Akses tidak sah), T02 (Malware), T05 (Human error), T08 (Pencurian perangkat), T09 (Kerusakan perangkat), T10 (Listrik padam)	32	High	A.7.13 Equipment Maintenance A.7.8 Equipment Siting and Protection
6	Pengelola Sistem Informasi	V02 - Kurangnya pelatihan atau pemahaman pengguna dalam penggunaan sistem informasi.	T01 (Akses tidak sah), T05 (Human error), T11 (Phishing)	30	Medium	A.6.3 Information Security Awareness, Education and Training
7	Pengguna Sistem Informasi	V02 - Kurangnya pelatihan atau pemahaman pengguna dalam penggunaan sistem informasi.	T01 (Akses tidak sah), T05 (Human error), T11 (Phishing)	30	Medium	A.6.3 Information Security Awareness, Education and Training
8	Layanan Web Hosting (Hostinger)	V09 - Pengujian pemulihan data cadangan belum dilakukan secara berkala.	T01 (Akses tidak sah), T02 (Malware), T03 (Kebocoran data), T06 (Gangguan layanan)	24	Low	A.8.13 Information Backup

Gambar 5. Penentuan Kontrol Keamanan Informasi (Aset Prioritas 1–8)

RINGKASAN: KERENTANAN, ANCAMAN & KONTROL ANNEX A – PER ASET (URUT PRIORITAS RISIKO)

No	Aset	Kerentanan (Vulnerability) Pemicu	Ancaman (Threat) Terkait	Risk Score	Level Risiko	Kontrol Annex A ISO/IEC 27001:2022
9	Modem	V04 - Pengamanan fisik terhadap perangkat belum optimal. V05 - Pemeliharaan dan pemantauan kondisi perangkat belum dilakukan secara berkala. V08 - Pemeriksaan kondisi jaringan dan perangkat jaringan belum dilakukan secara berkala.	T01 (Akses tidak sah), T06 (Gangguan layanan), T07 (Gangguan jaringan), T09 (Kerusakan perangkat), T10 (Listrik padam)	24	Low	A.7.13 Equipment Maintenance A.7.8 Equipment Siting and Protection A.8.20 Networks Security
10	Printer	V04 - Pengamanan fisik terhadap perangkat belum optimal. V05 - Pemeliharaan dan pemantauan kondisi perangkat belum dilakukan secara berkala.	T01 (Akses tidak sah), T05 (Human error), T08 (Pencurian perangkat), T09 (Kerusakan perangkat), T10 (Listrik padam)	20	Low	A.7.13 Equipment Maintenance A.7.8 Equipment Siting and Protection
11	LAN	V05 - Pemeliharaan dan pemantauan kondisi perangkat belum dilakukan secara berkala. V08 - Pemeriksaan kondisi jaringan dan perangkat jaringan belum dilakukan secara berkala.	T01 (Akses tidak sah), T06 (Gangguan layanan), T07 (Gangguan jaringan), T09 (Kerusakan perangkat)	20	Low	A.7.13 Equipment Maintenance A.8.20 Networks Security
12	AC	V05 - Pemeliharaan dan pemantauan kondisi perangkat belum dilakukan secara berkala.	T09 (Kerusakan perangkat), T10 (Listrik padam)	12	Very Low	A.7.13 Equipment Maintenance

Gambar 6. Penentuan Kontrol Keamanan Informasi (Aset Prioritas 9–12)

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Melalui hasil kajian, analisis risiko keamanan informasi pada PKBM XYZ memakai metode *Risk Assessment* berbasis ISO/IEC 27001:2022 berhasil mengidentifikasi aset teknologi informasi, ancaman, dan kerentanan yang memengaruhi keamanan informasi organisasi. Hasil penilaian menunjukkan bahwa setiap aset memiliki tingkat risiko yang berbeda berdasarkan kombinasi nilai *Likelihood* dan *Impact*. Aset laptop admin dan router berada pada tingkat risiko tertinggi sehingga menjadi prioritas utama dalam penerapan pengendalian keamanan informasi, sedangkan aset lainnya memiliki tingkat risiko yang bervariasi sesuai kondisi keamanan yang dimiliki. Berdasarkan hasil tersebut, rekomendasi kontrol keamanan yang mengacu pada Annex A ISO/IEC 27001:2022 disusun sebagai dasar mitigasi risiko dan diharapkan dapat membantu PKBM XYZ meningkatkan pengelolaan keamanan informasi secara lebih efektif.

B. Saran

Selanjutnya melalui hasil kajian yang telah dijalankan, bermacam saran yang mampu dibagikan yakni:

1. PKBM XYZ disarankan agar menjalankan rekomendasi kontrol keamanan yang telah diusulkan secara bertahap dengan memprioritaskan aset yang memiliki nilai risiko lebih tinggi agar upaya pengelolaan risiko dapat dilakukan secara lebih efektif.
2. Pengelolaan keamanan informasi perlu dilakukan secara berkelanjutan melalui pemantauan, evaluasi, dan

pembaruan terhadap aset, ancaman, serta kerentanan yang dapat berubah seiring perkembangan teknologi informasi dan kebutuhan organisasi.

3. PKBM XYZ disarankan untuk meningkatkan kesadaran keamanan informasi bagi seluruh pengelola maupun pengguna sistem melalui sosialisasi, pelatihan, dan penyusunan prosedur operasional yang mendukung penerapan keamanan informasi.

Penelitian berikutnya dimaksudkan mampu meningkatkan kajian ini dengan melakukan implementasi dan pengujian efektivitas kontrol menjalankan yang direkomendasikan, atau menggunakan standar maupun metode analisis risiko lainnya sebagai pembanding sehingga diperoleh hasil evaluasi yang lebih lengkap.

DAFTAR PUSTAKA

[1] Pratama, R. A., & Hidayat, T. (2023). Perancangan Sistem Manajemen Keamanan Informasi Berdasarkan ISO 27001:2022 (Studi Kasus: Data Center Diskominfo Kota Tangerang Selatan). Jurnal Sistem Informasi, 12(2), 45–58.

[2] Humphreys, E. (2022). *Implementing the ISO/IEC 27001:2022 ISMS Standard (3rd ed.)*. Artech House.

[3] Stamp, M. (2021). *Information Security: Principles and Practice (3rd ed.)*. Wiley.

[4] Stallings, W., & Brown, L. (2021). *Computer Security: Principles and Practice (5th ed.)*. Pearson.

[5] Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security (7th ed.)*. Cengage Learning.

[6] International Organization for Standardization. (2022). *ISO/IEC 27001:2022 — Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems —* Requirements. ISO.

[7] Calder, A. (2022). *ISO 27001/ISO 27002: A Pocket Guide (3rd ed.)*. IT Governance Publishing.

[8] National Institute of Standards and Technology. (2018). *NIST SP 800-30 Rev. 1 — Guide for Conducting Risk Assessments*. U.S. Department of Commerce.

[9] Ardius, E., & Syamsuar, D. (2023). *Assessment Risk* terhadap Penggunaan Sistem Informasi Akademik Universitas EA Menggunakan Metode ISO 27001. Jurnal Teknologi Informasi Mura, 15(1), 4-6.

[10] Putri, A. N., & Saputra, R. (2023). Analisis Manajemen Risiko terhadap Pelayanan Peminjaman Aset Barang Program Studi Teknik Informatika Menggunakan ISO 27001:2022. Jurnal Rekayasa Sistem Informasi, 5(3), 78–89.

[11] Permatasari, D., & Nugroho, E. (2022). Penerapan Sistem Manajemen Keamanan Informasi ISO 27001 pada Perpustakaan Nasional Republik Indonesia. Jurnal Ilmu Perpustakaan dan Informasi, 7(1), 33–42.

[12] Miles, M. B., Huberman, A. M., & Saldaña, J. (2020). *Qualitative Data Analysis: A Methods Sourcebook (4th ed.)*. SAGE Publications.

LAMPIRAN

TABEL 10. Kuesioner Wawancara

No.	Kode	Nilai	Pernyataan	Hasil Wawancara
1	Q1	2	PKBM XYZ telah memiliki kebijakan atau aturan yang mengatur keamanan informasi yang digunakan dan dikelola oleh organisasi.	Aturan keamanan informasi belum tertuang dalam dokumen SOP formal, namun instruksi dan imbauan dasar sudah disampaikan secara lisan oleh pemilik kepada pengelola.
2	Q2	2	Peran dan tanggung jawab pihak yang mengelola sistem informasi dan keamanan informasi telah ditetapkan dengan jelas.	Pembagian tugas teknis belum diatur dalam Struktur Organisasi resmi; penanganan sistem masih dirangkap oleh staf administrasi berdasarkan kebiasaan (informal).
3	Q3	3	Terdapat aturan mengenai penggunaan aset informasi dan aset TI yang digunakan dalam kegiatan PKBM XYZ.	Sudah terdapat tata tertib/SOP tertulis mengenai pemanfaatan inventaris komputer dan jaringan internet yang ditempel di ruang operasional.
4	Q4	4	Akses terhadap sistem informasi dan informasi diberikan sesuai dengan kebutuhan dan kewenangan pengguna.	Sistem telah memiliki tingkatan *user role* (Admin, Pengajar, Siswa). Pembatasan hak akses berjalan konsisten sesuai fungsi dan tugas masing-masing.
5	Q5	4	Hak akses pengguna terhadap sistem informasi ditinjau dan diperbarui apabila terjadi perubahan kebutuhan atau kewenangan.	Peninjauan hak akses dilakukan secara berkala; akun staf/pengajar yang sudah tidak aktif langsung dicabut atau dinonaktifkan oleh pengelola.
6	Q6	4	Penggunaan layanan *web hosting* yang mendukung sistem informasi dikelola dengan mempertimbangkan aspek keamanan informasi.	Layanan *web hosting* disewa dari penyedia terpercaya yang sudah mencakup perlindungan SSL/HTTPS, *auto-backup*, dan fitur keamanan standar.
7	Q7	3	Pengelola dan pengguna sistem informasi telah memperoleh edukasi atau pelatihan mengenai keamanan informasi sesuai dengan perannya.	Pengelola telah mengikuti pengarahan dasar mengenai literasi digital dan keamanan data, meski pelatihan tingkat lanjut belum terprogram secara rutin.
8	Q8	2	Pengelola dan pengguna sistem informasi mengetahui cara melaporkan kejadian atau dugaan insiden keamanan informasi yang terjadi.	Belum ada formulir atau alur penanganan insiden tertulis; pelaporan kendala/gangguan keamanan masih dilakukan secara langsung lewat pesan WhatsApp ke pengelola.
9	Q9	2	Perangkat TI yang digunakan untuk mendukung sistem informasi dilindungi dari akses fisik yang tidak berwenang.	Perangkat komputer berada di ruang administrasi publik; saat jam istirahat atau luar jam kerja, perlindungan fisik baru mengandalkan penguncian pintu ruangan secara umum.
10	Q10	2	Perangkat TI dilindungi dari risiko lingkungan	Ruangan sudah dilengkapi pendingin udara (AC), namun belum

			seperti gangguan suhu, listrik, dan kondisi lingkungan lain yang dapat mengganggu operasional perangkat.	dilengkapi proteksi kelistrikan tambahan seperti UPS (*Uninterruptible Power Supply*) atau stabilizer.
11	Q11	2	Perangkat TI dipelihara secara berkala untuk menjaga ketersediaan dan keamanan perangkat.	Pemeliharaan perangkat keras maupun pembersihan sistem belum memiliki jadwal rutin, perbaikan baru dilakukan jika terjadi kerusakan.
12	Q12	2	Kerentanan teknis pada sistem dan perangkat endpoint diidentifikasi dan ditangani secara berkala.	Pembaruan sistem (*update* OS/*software*) dan pemindaian virus dilakukan secara manual bila timbul kelambatan/masalah pada perangkat, belum ada pemindaian rutin.
13.	Q13	4	Perangkat *endpoint* yang digunakan untuk mengakses atau mengelola informasi telah memiliki perlindungan terhadap *malware* dan dilakukan pemeriksaan atau pembaruan secara berkala.	Perangkat *endpoint* yang digunakan untuk mengakses dan mengelola sistem informasi memiliki perlindungan terhadap *malware*.
14.	Q14	3	Informasi penting pada sistem informasi dicadangkan secara berkala melalui mekanisme pencadangan yang dapat digunakan untuk pemulihan apabila terjadi kehilangan atau kerusakan data.	Informasi pada sistem informasi dicadangkan melalui mekanisme *auto-backup* yang tersedia pada layanan web *hosting*. Selain itu, pencadangan *database* juga dilakukan secara manual. Pemantauan terhadap hasil *auto-backup* dan pencadangan manual *database* dilakukan setiap dua minggu sekali.
15.	Q15	2	Aktivitas dan kejadian yang relevan dengan keamanan sistem dan perangkat TI dipantau serta ditinjau secara berkala.	*Monitoring* dan *logging* keamanan sistem belum memiliki jadwal peninjauan rutin.