SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

PERENCANAAN SMKI BERDASARKAN ISO/IEC 27001:2022 PADA PONDOK YATIM DHUAFA THURSINA BOGOR

TUGAS AKHIR

Sri Auliani Trisna

0110120034

PROGRAM STUDI SISTEM INFORMASI

SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

DEPOK

AGUSTUS 2024

SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

PERENCANAAN SMKI BERDASARKAN ISO/IEC 27001:2022 PADA PONDOK YATIM DHUAFA THURSINA BOGOR

TUGAS AKHIR

Sri Auliani Trisna

0110120034

PROGRAM STUDI SISTEM INFORMASI

SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

DEPOK

AGUSTUS 2024

HALAMAN PERNYATAAN ORISINALITAS

Skripsi/Tugas Akhir ini adalah hasil karya penulis, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : **Sri Auliani Trisna**

NIM : **0110120034**

Depok, 05 Agustus 2024

Tanda Tangan

Sri Auliani Trisna

HALAMAN PENGESAHAN

Skripsi/Tugas Akhir ini diajukan oleh :

Nama : Sri Auliani Trisna

NIM : 0110120034

Program Studi : Sistem Informasi

Judul Skripsi : Perencanaan Sistem Manajemen Keamanan Informasi Berdasarkan ISO/IEC 27001: 2022 Pada Pondok Yatim Dhuafa Thursina Bogor

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana S1 pada Program Studi Sistem Informasi Sekolah Tinggi Teknologi Terpadu Nurul Fikri

DEWAN PENGUJI

Pembimbing	Penguji
	1/8/24
Drs. Rusmanto, M.M.	Suhendi, S.T., S.Kom., M.M.S.I.

Ditetapkan di : Depok

Tanggal : 05 Agustus 2024

KATA PENGANTAR

Alhamdulillah, puji syukur atas kehadirat Allah SWT, berkat dan rahmat Nya penulis dapat menyelesaikan tugas akhir ini. Penulisan skripsi/Tugas Akhir ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana komputer Program Studi Sistem Informasi pada Sekolah Tinggi Teknologi Terpadu Nurul Fikri Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi penulis untuk menyelesaikan skripsi/tugas akhir ini. Oleh karena itu, penulis mengucapkan terima kasih kepada :

1. Allah SWT, atas nikmat yang begitu luar biasa yang diberikan kepada penulis sebagai hambaNya.
2. Nabi Muhammad SAW, atas berkah shalawat kepadaNya. Hingga nanti semoga mendapatkan syafaat di yaumul akhir.
3. Cinta pertama ku, Ayahanda Ade Trisna Mandayani dan pintu surgaku Ibu Didoh Nuridoh. Terima kasih atas pengorbanan dan kasih sayangnya. Yang selalu mendoakan dan dukungan hingga penulis mampu menyelesaikan studinya sampai sarjana. Semoga Ayah dan Ibu sehat, berkah umur dan bahagia selalu.
4. Saudara dan saudariku yang tak kalah penting kehadirannya, Teh Ika, A Ropik, Teh Mia, Ka Mujib, Adik Saftina, Azmiy, Radhwa, dan Alm. Dhavitha, serta 3 keponakan ku, Ikram, Arkan, dan Sakhiy. Terima kasih telah menjadi bagian dari perjalanan penulis. Berkontribusi dalam proses karya tulis ini baik waktu dan tenaga, dalam mendukung, menghibur, dan mengajarkan arti kesabaran.
5. Bapak Dr. Lukman Rosyidi, M.M., M.T., sebagai Ketua Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
6. Ibu Misna Asqia, M.Kom., sebagai Ketua Program Studi Sistem Informasi Sekolah Tinggi Teknologi Terpadu Nurul Fikri.

7. Drs. Rusmanto, M.M., sebagai Dosen Pembimbing, yang telah memberikan arahan, ilmu, dan dukungan kepada penulis selama proses penyusunan tugas akhir ini.
8. Para Dosen di lingkungan Sekolah Tinggi Teknologi Terpadu Nurul Fikri yang telah membimbing penulis dalam menuntut ilmu.
9. Bapak Ikbar Muhyi Maulani, S.Kom., M.Pd., sebagai Ketua Pimpinan Pondok Yatim Dhuafa Thursina yang telah memberikan kesempatan untuk melakukan penelitian dan membantu dalam memberikan data yang diperlukan bagi penulisan ilmiah ini.
10. Teman kelas Sistem Informasi 03, keluarga besar LDK Senada, dan teman kampusku lainnya yang telah memberikan semangat dan dukungan selama menjalani perkuliahan ini.
11. Sahabatku (Olis, fiqih, Cindy, Intan, Mayang, Caca, Ega, Millah) yang telah membersamai dalam banyak hal.
12. Untukmu yang tertulis dalam *Lauhil Mahfudz*, terima kasih atas kekuatan doamu kepada penulis, semoga kita bisa mejadi partner dunia sampai surgaNya. Dan sampai bertemu di waktu yang tepat, untuk membangun keluarga yang Sakinah Mawaddah Warahmah.
13. Terakhir, untuk diriku sendiri, Sri Auliani Trisna atas segala kerja keras dan semangatnya sehingga tidak menyerah dan bisa menyelesaikan tugas akhir ini. Terima kasih sudah kuat dan bisa bertahan sampai saat ini, dan kedepannya bisa lebih kuat, sehat, bahagia dunia sampai surga dan bisa mewujudkan cita citanya.

Dalam penulisan ilmiah ini, masih terdapat kekurangan yang mungkin disebabkan oleh keterbatasan pengetahuan dan kemampuan penulis. Walaupun begitu, penulis telah berupaya semaksimal mungkin untuk menyelesaikan karya ini. Oleh karena itu, apabila terdapat kekurangan dalam karya ilmiah ini, penulis dengan tulus menerima masukan dan saran dari pembaca. Penulis berharap agar Tuhan memberkahi segala kebaikan semua pihak yang telah membantu. Semoga karya ini dapat memberikan manfaat bagi perkembangan ilmu.

Depok, 05 Agustus 2024

Sri Auliani Trisna

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI

TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Sekolah Tinggi Teknologi Terpadu Nurul Fikri, saya yang bertanda tangan di bawah ini:

Nama : Sri Auliani Trisna

NIM : 0110120034

Program Studi : Sistem Informasi

Jenis karya : Skripsi / Tugas Akhir

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada STT NF **Hak Bebas Royalti Non Eksklusif (*Non-exclusive Royalty - Free Right*)** atas karya ilmiah saya yang berjudul :

Perencanaan Sistem Manajemen Keamanan Informasi Berdasarkan ISO/IEC 27001:2022 Pada Pondok Yatim Dhuafa Thursina Bogor

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini STT-NF berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok

Pada tanggal : 05 Agustus 2024

Yang Menyatakan

Sri Auliani Trisna

ABSTRAK

Nama : Sri Auliani Trisna
NIM : 0110120034
Program Studi : Sistem Informasi
Judul : Perencanaan Sistem Manajemen Keamanan Informasi Berdasarkan ISO/IEC 27001:2022 Pada Pondok Yatim Dhuafa Thursina Bogor

Perkembangan teknologi informasi telah berdampak signifikan pada berbagai sektor, termasuk organisasi nirlaba yang menghadapi tantangan keamanan informasi. Pondok Yatim Dhuafa Thursina Bogor, misalnya, berisiko mengalami kebocoran data sensitif tanpa sistem manajemen keamanan informasi (SMKI) yang memadai. ISO/IEC 27001:2022 menyediakan kerangka kerja untuk mengatasi masalah ini dengan meningkatkan keamanan data dan kepercayaan donatur. Penelitian ini bertujuan merancang dan mengimplementasikan SMKI berbasis ISO/IEC 27001:2022 di Pondok Yatim Dhuafa Thursina Bogor. Pengelolaan risiko keamanan di Pondok Yatim Dhuafa Thursina Bogor dilakukan sesuai dengan standar ISO/IEC 27001:2022, mencakup identifikasi, analisis, dan evaluasi risiko yang terstruktur. Hasil penelitian menunjukkan, Pondok Yatim Dhuafa Thursina Bogor dapat mengidentifikasi dan mengevaluasi risiko keamanan informasi secara efektif, serta menyusun langkah mitigasi yang tepat. Penerapan standar ini membantu lembaga dalam menjaga keamanan informasi yang dikelola. Evaluasi menunjukkan bahwa langkah-langkah yang diterapkan memenuhi kebutuhan lembaga dan menekankan pentingnya pengujian serta pemantauan berkelanjutan. Dengan mengikuti standar ISO/IEC 27001:2022, lembaga ini dapat meningkatkan perlindungan informasi sensitif, memperkuat kepercayaan, dan reputasi di mata donatur dan masyarakat.

Kata kunci : Teknologi Informasi, SMKI, ISO/IEC 27001:2022, Keamanan Informasi, Pondok Yatim Dhuafa Thursina.

ABSTRACT

Name : Sri Auliani Trisna
NIM : 0110120034
Study Program : Information Systems
Title : Information Security Management System Planning Based on ISO / IEC 27001: 2022 at Pondok Yatim Dhuafa Thursina Bogor

The development of information technology has had a significant impact on various sectors, including non-profit organizations that face information security challenges. Pondok Yatim Dhuafa Thursina Bogor, for example, is at risk of sensitive data being leaked without an adequate information security management system (ISMS). ISO/IEC 27001:2022 provides a framework to address these issues by improving data security and donor trust. This research aims to design and implement ISMS based on ISO/IEC 27001:2022 at Pondok Yatim Dhuafa Thursina Bogor. Security risk management at Pondok Yatim Dhuafa Thursina Bogor is carried out in accordance with the ISO/IEC 27001:2022 standard, including structured risk identification, analysis and evaluation. The research results show that Pondok Yatim Dhuafa Thursina Bogor can identify and evaluate information security risks effectively, as well as develop appropriate mitigation steps. Implementing these standards helps institutions maintain the security of the information they manage. The evaluation demonstrated that the measures implemented met the agency's needs and emphasized the importance of ongoing testing and monitoring. By following the ISO/IEC 27001:2022 standard, this institution can improve the protection of sensitive information, strengthening trust and reputation in the eyes of donors and the public.

Keywords: Information Technology, ISMS, ISO/IEC 27001:2022, Information Security, Pondok Yatim Dhuafa Thursina.

DAFTAR ISI

STT - NF

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi telah membawa dampak signifikan dalam berbagai sektor, termasuk pada organisasi atau institusi nirlaba. Penggunaan teknologi dalam pengelolaan data dan informasi menjadi krusial untuk meningkatkan efisiensi dan keberlanjutan operasional lembaga-lembaga tersebut. Namun, sering kali organisasi nirlaba menghadapi tantangan terkait keamanan informasi yang tidak dapat diabaikan. Sebagai contoh, sebuah pondok yatim dan dhuafa mungkin menghadapi risiko kebocoran data sensitif anak asuh atau donatur jika tidak dilengkapi dengan sistem manajemen keamanan informasi (SMKI) yang memadai. Selain itu, tuntutan regulasi dan standar internasional semakin menekankan pentingnya praktik keamanan informasi yang baik.

Pondok Yatim Dhuafa Thursina Bogor merupakan salah satu institusi yang berperan penting dalam memberikan bantuan dan pendidikan kepada anak-anak yatim dan dhuafa. Sebagai lembaga yang menyimpan dan mengelola berbagai data sensitif, baik data keuangan maupun data pribadi anak asuh dan donatur, keamanan informasi menjadi aspek krusial untuk diimplementasikan. Pada situasi terkini menunjukkan bahwa banyak lembaga sejenis, termasuk Pondok Yatim Dhuafa Thursina, masih menghadapi tantangan signifikan dalam mengelola sistem manajemen keamanan informasi (SMKI) secara efektif.

Sebagai contoh, banyak lembaga sosial dan pendidikan di Indonesia belum menerapkan standar internasional dalam manajemen keamanan informasi, menyebabkan rentannya data terhadap ancaman siber. Penelitian oleh Fauzi *et al.* (2019) mengungkapkan bahwa kurangnya pemahaman dan sumber daya menjadi hambatan utama dalam implementasi SMKI [1]. Hal ini menunjukkan adanya kesenjangan antara kondisi ideal yang seharusnya dapat dicapai, yaitu adanya SMKI yang kokoh dan terstandarisasi, dengan kondisi faktual yang terjadi di lapangan.

ISO/IEC 27001:2022 adalah standar internasional terbaru untuk manajemen keamanan informasi yang menyediakan kerangka kerja untuk merancang, mengimplementasikan, mengelola, memantau, dan memperbaiki SMKI. Standar ini membantu organisasi dalam mengamankan aset informasinya dengan cara yang sistematis dan terstruktur [2]. Penerapan ISO/IEC 27001:2022 dapat menjadi solusi rasional untuk mengatasi masalah keamanan informasi di berbagai organisasi, termasuk Pondok Yatim Dhuafa Thursina Bogor.

Studi oleh Tsohou et al. (2020) menekankan pentingnya alih teknologi dan pengetahuan dalam menerapkan standar keamanan informasi di berbagai organisasi pendidikan dan sosial, yang seringkali beroperasi dengan keterbatasan sumber daya. Implementasi standar ini tidak hanya melibatkan aspek teknis dan operasional, tetapi juga perubahan budaya dan perilaku kerja dalam organisasi. Ini termasuk pelatihan, kesadaran, dan komunikasi yang efektif mengenai pentingnya keamanan informasi [3].

Pondok Yatim Dhuafa Thursina Bogor, dengan keterbatasannya, sejauh ini belum secara maksimal menggunakan praktik-praktik terbaik dalam keamanan informasi. Mengikuti kerangka kerja ISO/IEC 27001:2022, lembaga ini diharapkan mampu meningkatkan keamanan data, serta meningkatkan reputasi dan kepercayaan donatur serta pelindungnya. Menurut penelitian yang dilakukan oleh Smith dan Brooks (2021), institusi yang berhasil menerapkan ISO/IEC 27001:2022 mengalami peningkatan kepercayaan klien dan *stakeholder*, serta penurunan insiden keamanan [4].

Dengan demikian, perencanaan SMKI yang komprehensif dan berdasarkan standar internasional menjadi solusi logis dan diperlukan untuk Pondok Yatim Dhuafa Thursina. Penelitian ini bertujuan untuk merancang dan menerapkan sistem manajemen keamanan informasi berbasis ISO/IEC 27001:2022 untuk meningkatkan efektivitas pengelolaan informasi di Pondok tersebut. Dan penulis berharap dapat memperoleh pemahaman tentang perencanaan SMKI. Adapun judul yang diangkat untuk penelitian ini yaitu "**PERENCANAAN SMKI BERDASARKAN ISO/IEC 27001:2022 PADA PONDOK YATIM DHUAFA THURSINA BOGOR".**

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan sebelumnya, maka diperoleh rumusan permasalahan yaitu :

1. Bagaimana pengelolaan risiko terkait keamanan, yang mencakup identifikasi risiko, analisis penilaian risiko, dan evaluasi risiko terkait sistem manajemen keamanan informasi (SMKI) sesuai dengan standar ISO/IEC 27001:2022 di Pondok Yatim Dhuafa Thursina Bogor?
2. Bagaimana evaluasi hasil pengelolaan risiko terkait keamanan, yang mencakup identifikasi risiko, analisis penilaian risiko, dan evaluasi risiko terkait sistem manajemen keamanan informasi (SMKI) sesuai dengan standar ISO/IEC 27001:2022 di Pondok Yatim Dhuafa Thursina Bogor?

1.3 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah :

1. Memahami pengelolaan risiko terkait keamanan, yang mencakup identifikasi risiko, analisis penilaian risiko, dan evaluasi risiko terkait sistem manajemen keamanan informasi (SMKI) sesuai dengan standar ISO/IEC 27001:2022 di Pondok Yatim Dhuafa Thursina Bogor.
2. Memahami proses evaluasi hasil pengelolaan terkait keamanan, yang mencakup identifikasi risiko, analisis penilaian risiko, dan evaluasi risiko terkait sistem manajemen keamanan informasi (SMKI) sesuai dengan standar ISO/IEC 27001:2022 di Pondok Yatim Dhuafa Thursina Bogor.

1.4 Manfaat Penelitian

1. Mengetahui lebih banyak tentang proses perencanaan sistem manajemen keamanan informasi dan apa yang harus dilakukan pada setiap tahapnya.
2. Mengetahui dan membantu dalam menemukan, menganalisis,dan mengelola risiko masalah terkait sistem manajemen keamanan informasi dan meningkatkan keamanan sistem informasi PYDT.

1.5 Batasan Masalah

1. Penelitian ini berupa pengelolaan risiko terkait keamanan, yang mencakup identifikasi risiko, analisis penilaian risiko, dan evaluasi risiko sehingga tidak mencakup kegiatan penanganan risiko, hanya evaluasi risiko dengan memberikan rekomendasi penanganan risiko.
2. Penelitian ini hanya mencakup perencanaan Sistem Manajemen Keamanan Informasi berdasarkan ISO/IEC2 27001:2022. Implementasi atau evaluasi dari penerapan SMKI tidak termasuk dalam penelitian ini.
3. Pengumpulan data dan informasi akan dibatasi pada data yang tersedia dan dapat diakses selama periode penelitian.
4. Penelitian ini akan menggunakan metode kualitatif dengan pendeketan studi kasus.

1.6 Sistematika Penulisan

1. Bab I Pendahuluan : Bab ini merupakan gambaran umum dari topik yang akan dibahas seperti latar belakang, identifikasi masalah, perumusan masalah, batasan masalah, tujuan penelitian, ruang lingkup, dan manfaat dari penelitian, serta tahap dan kegiatan penelitian.
2. Bab II Kajian Literatur : Bab ini merupakan penjelasan terkait teori-teori dan referensi pada pengolahan data, sistem informasi, SMKI, ISO/IEC 27001:2022, Risiko Manajemen dan beberapa teori yang digunakan sebagai pendukung pada penelitian ini.
3. Bab III Metode Penelitian : Pada bab penelitian ini akan membahas tentang tahapan proses perencanaan pada SMKI, jenis penelitian, metode penyelesaian masalah, pengumpulan data, analisis kebutuhan, dan perencanaan sistem.
4. Bab IV Hasil dan Pembahasan : Bab ini merupakan uraian yang akan dibahas dari hasil penelitian dari metode yang digunakan pada bab sebelumnya.

5. Bab V Kesimpulan dan Saran : Bab ini berisi jawaban atau menjawab pertanyaan dari rumusan masalah hingga dapat hasil penelitian pada laporan akhir dan saran yang dapat dilakukan untuk penelitian selanjutnya.

BAB II
KAJIAN LITERATUR

2.1 Profil Pondok Yatim dan Dhuafa Thursina Bogor

2.1.1 Studi Pendahuluan

Pondok Yatim Dhuafa Thursina merupakan lembaga kesejahteraan sosial anak di bawah naungan Departemen Sosial. PYD Thursina berasal dari LAZIS PT PLN Kantor Pusat, yang dibentuk pada tanggal 11 September 2006 berdasarkan keputusan Direksi Nomor 132.K/DIR/2006. Tujuan PYD Thursina adalah mengelola dana zakat, infaq, dan shodaqoh dari pegawai PLN Pusat. Sebelumnya dikenal dengan nama Pondok Yatim Dhuafa YBM PLN, salah satu dari pondok ini didirikan atas dorongan Wakif bernama Hj. Imas Fatimah. Beliau mendasarkan tindakannya pada ajaran agama Islam, yang mengajarkan pentingnya tolong-menolong sesama. Hj. Imas Fatimah melihat banyak anak yang kurang beruntung secara finansial dan tidak bisa mengakses pendidikan. Dengan rezeki yang diterimanya, beliau merasa mampu membantu mereka yang membutuhkan [5]. Berikut ini merupakan visi, misi, dan tujuan dari Pondok Yatim Dhuafa Thursina :

a. Visi

   "Sebagai lembaga kesejahteraan sosial anak yang memiliki keunggulan nilai-nilai keislaman, mandiri dan berintegritas".

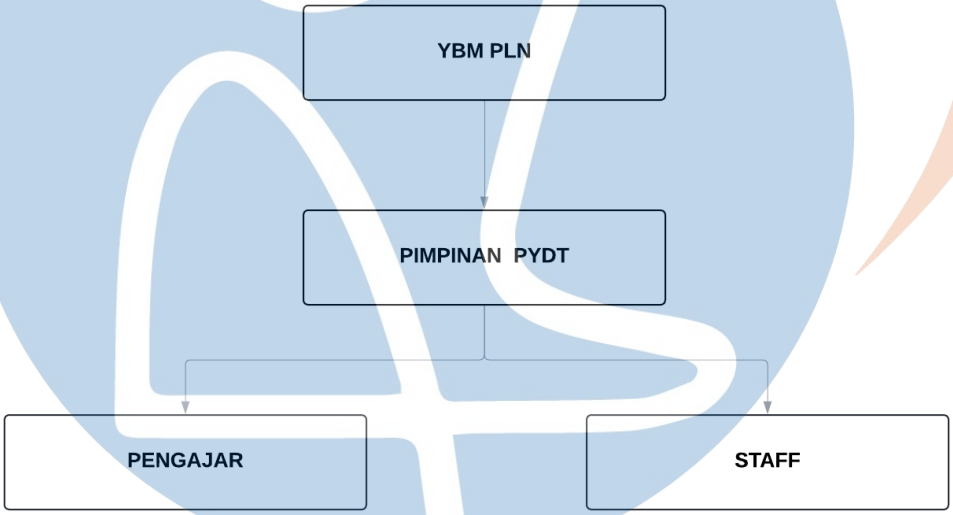
b. Misi

   1. Menerapkan nilai – nilai keislaman yang baik dan benar.
   2. Pola pendampingan berbasis pesantren.
   3. Menggunakan metode-metode terbaik dalam menghafalkan al qur'an.
   4. Mencetak alumni yang memiliki hafalan minimal 5 juz dan berdaya saing di bidang keagamaan.
   5. Mengaplikasikan pola hidup sehat dan bersih.

c. Tujuan

1. Mencetak anak generasi muslim tangguh yang hanief (berpihak kepada kebenaran), cageur (sehat), bageur (shalih/ baik / berakhlak karimah), bener (jujur dan berintegritas), pintar (cerdas).
2. Menghadirkan pendidikan dan pengajaran serta pendampingan dengan muatan keislaman.
3. Berkemampuan membaca dan menghafal Qur'an dengan baik.
4. Mempersiapkan alumni sebagai anak yang mandiri dan tangguh.

2.1.2 Struktur Organisasi



Gambar 2. 1 Struktur Organisasi PYD Thursina

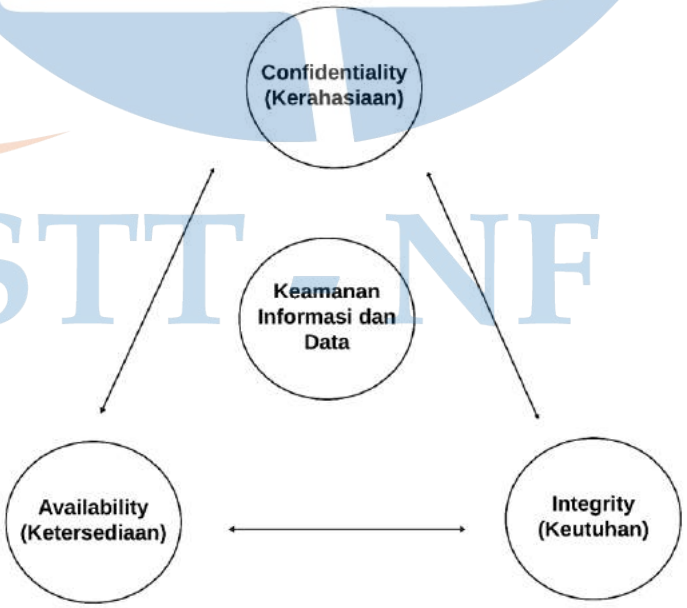
2.2 Sistem Informasi

Sistem informasi adalah gabungan dari perangkat keras, perangkat lunak, dan manusia yang bekerja sama untuk mengelola data menggunakan teknologi yang ada. Data juga memiliki peran yang sangat vital dalam sistem informasi, di mana data yang dimasukkan bisa berupa formulir, prosedur, atau jenis data lainnya. Pada sisi lain, informasi adalah hasil dari pengolahan data yang dapat memberikan manfaat yang lebih besar bagi penggunanya. Data yang telah diolah untuk menghasilkan wawasan yang lebih bermanfaat dalam mencapai tujuan tertentu disebut sebagai

informasi [6]. Informasi dianggap bermanfaat apabila memberikan manfaat yang signifikan daripada sekadar menampilkan data. Untuk sebuah sistem dianggap berhasil, sistem tersebut harus mencapai tujuan yang telah ditetapkan. Tujuan yang telah ditetapkan akan menentukan *input* dan *output* yang diperlukan oleh sistem tersebut [12].

2.3 Keamanan Informasi

Keamanan informasi adalah usaha untuk memastikan bahwa informasi, baik tertulis, lisan, elektronik, atau grafis, aman. Kerahasiaan, aksesibilitas, dan ketersediaan data atau informasi adalah tujuan utama keamanan data. Selain itu, mereka berusaha untuk menghindari kerusakan, kehilangan, atau penyebaran data pribadi kepada pihak yang tidak berwenang. Salah satunya adalah upaya untuk meminimalkan risiko bisnis, mempercepat pengambilan investasi, dan menjamin kelangsungan bisnis [7]. Keberlanjutan Teknologi Informasi (TI) sangat penting bagi organisasi untuk mencapai tujuan bisnisnya. Keberlanjutan Teknologi Informasi sangat bergantung pada efektivitas keamanan informasi dalam organisasi untuk memastikan Kerahasiaan, Integritas, dan Ketersediaan yang sering disebut sebagai 3 elemen keamanan informasi CIA.



Gambar 2. 2 Tiga Elemen Keamanan Informasi (CIA)

1. *Confidentiality* (Kerahasiaan) : Data sensitif dan harus dilindungi agar orang yang tidak memiliki hak untuk mengaksesnya tidak dapat mengaksesnya.
2. *Integrity* (Keutuhan) : Keamanan informasi berarti menjaga layanan, kelengkapan, dan keamanan informasi dari kehilangan, kerusakan, dan ancaman lainnya.
3. *Availability* (Ketersediaan) : Informasi harus lengkap dan tidak dapat berubah. Di mana informasi harus terjamin ketersediaannya dan mendukung semua proses dalam informasi yang dibutuhkan oleh pengguna yang selalu tersedia kapan pun.

Hal ini memungkinkan informasi tersebut dapat diakses dan digunakan dengan cepat oleh pengguna yang berhak. Dalam mengelola aspek keamanan informasi CIA, organisasi perlu mengadopsi pendekatan yang komprehensif dan berkelanjutan. Keberlanjutan TI melibatkan penggunaan teknologi informasi yang berkelanjutan, pemantauan yang efektif terhadap ancaman keamanan informasi, serta pemeliharaan dan perbaikan yang terus-menerus terhadap sistem TI. Selain itu, penerapan kebijakan keamanan informasi, keterlibatan karyawan dalam praktik keamanan informasi, dan evaluasi berkala terhadap kebijakan dan praktik yang ada juga merupakan faktor penting dalam menjaga keberlanjutan TI organisasi. Dengan memastikan keberlanjutan TI yang efektif melalui manajemen keamanan informasi yang baik, organisasi dapat mengurangi risiko pelanggaran data, kerugian finansial, dan kerugian reputasi. Keberlanjutan TI yang baik juga dapat mendukung inovasi dan transformasi digital organisasi, serta meningkatkan kepercayaan pelanggan dan mitra bisnis terhadap organisasi. Dalam konteks perkembangan teknologi dan ancaman terhadap keamanan informasi, beberapa ahli keamanan informasi telah mengusulkan tambahan atau pengembangan dari prinsip Kerahasiaan, Integritas, dan Ketersediaan (CIA). Salah satu alternatif aspek keamanan informasi yang diajukan oleh *Rhodes-Ousley* adalah Parkerian *Hexad* yang terdiri dari CIA ditambah dengan kontrol, keaslian, dan utilitas. Selain itu, prinsip lain yang pernah diusulkan meliputi Akuntabilitas, *Non-Reputability*, dan Legalitas. Departemen

Pertahanan Amerika Serikat juga telah menetapkan 5 pilar jaminan informasi yang mencakup CIA serta keaslian dan *Non-Reputability* sebagai aspek keamanan informasi yang penting. Selanjutnya, *Organization for Economic Co-operation and Development* (OECD) telah menerbitkan panduan yang menambahkan beberapa aspek keamanan informasi, seperti kesadaran, tanggung jawab, respons, etika, demokrasi, penilaian risiko, desain dan implementasi keamanan, manajemen keamanan, serta penilaian ulang.

2.4 Aset

Aset adalah kekayaan yang dimiliki oleh suatu lembaga atau segala hak yang bisa dimanfaatkan di dalam lembaga tersebut. Aset yang didefinisikan sebagai sistem manajemen keamanan informasi (SMKI) adalah segala sesuatu yang berharga bagi organisasi dan harus dijaga. Untuk memastikan kerahasiaan, integritas, dan ketersediaan informasi, keamanan aset adalah tujuan utama SMKI. Aset dapat berupa informasi, perangkat keras, perangkat lunak, infrastruktur, manusia, dan reputasi.

2.5 Metode Kualitatif

Metode kualitatif adalah pendekatan penelitian yang bertujuan untuk memahami fenomena kompleks melalui pengumpulan dan analisis data non-numerik. Data ini dapat mencakup wawancara, observasi, dan analisis dokumen yang semuanya memeberikan wawasan mendalam tentang konteks, perspektif partisipan, dana proses sosial yang berlangsung dalam suatu setting. Metode kualitatif sangat berguna untuk mengeksplorasi isu-isu yang belum banyak diteliti atau untuk memahami dinamika dan interaksi yang rumit dalam konteks sosial tertentu. Karakteristik utama metode kualitatif meliputi:

1. Pendekatan Holistik: Penelitian kualitatif memandang fenomena secara keseluruhan dalam konteks alaminya. Peneliti mengumpulkan data secara rinci dan berfokus pada pemahaman mendalam tentang subjek penelitian.

2. Data *Non-Numerik*: Metode ini mengandalkan data non-numerik seperti wawancara, observasi, dan analisis teks. Data tersebut dianalisis untuk mengidentifikasi tema, pola, dan kategori.
3. Analisis Induktif: Pendekatan kualitatif sering menggunakan analisis induktif, di mana peneliti mengembangkan teori dan konsep berdasarkan data yang dikumpulkan, bukan menguji hipotesis yang telah ditetapkan sebelumnya.
4. Interaksi Peneliti dan Partisipan: Peneliti kualitatif sering terlibat langsung dengan partisipan dan lingkungan mereka, yang memungkinkan mereka mendapatkan wawasan lebih dalam tentang konteks sosial dan budaya yang sedang diteliti.

Metode kualitatif sangat bermanfaat dalam penelitian yang bertujuan untuk mendapatkan pemahaman mendalam tentang fenomena sosial dan perilaku manusia, terutama dalam konteks di mana data kuantitatif mungkin tidak cukup memadai untuk memberikan gambaran yang lengkap [17].

2.6 ISO 27001:2022 Sistem Manajemen Keamanan Informasi

ISO/IEC 27001:2022 adalah standar internasional terbaru untuk manajemen keamanan informasi yang menyediakan kerangka kerja sistematis dan terstruktur untuk merancang, mengimplementasikan, mengelola, memantau, dan memperbaiki SMKI. Standard ini membantu organisasi dalam mengamankan aset informasi mereka dengan cara yang lebih efektif dan efisien (ISO/IEC, 2022).

Penerapan standar ini dianggap sebagai solusi rasional dalam mengatasi masalah keamanan informasi di berbagai organisasi. Menurut *Smith* dan *Brooks* (2021), institusi yang berhasil menerapkan ISO/IEC 27001:2022 cenderung mengalami peningkatan kepercayaan dari klien dan *stakeholder* mereka serta penurunan insiden keamanan. Penelitian ini menunjukkan bahwa penerapan standar ISO/IEC 27001:2022 tidak hanya meningkatkan keamanan data tetapi juga reputasi dan kepercayaan lembaga [4].

Standar ISO 27001:2022 didasarkan pada pendekatan manajemen risiko yang melibatkan pemahaman mendalam tentang lingkungan bisnis organisasi dan

evaluasi sumber daya dan proses yang terlibat dalam sistem manajemen keamanan informasi. Proses ini bertujuan untuk mengidentifikasi potensi risiko keamanan informasi. Setelah risiko diidentifikasi, organisasi menilai setiap risiko dan mengevaluasi potensi dampak yang mungkin terjadi. Organisasi kemudian mengembangkan strategi manajemen risiko untuk mengurangi risiko keamanan informasi yang teridentifikasi. Penerapan standar ISO 27001 memerlukan keterlibatan luas dari manajemen dan personel operasional organisasi. Seluruh proses perencanaan, pelaksanaan, pemantauan, evaluasi, dan perbaikan sistem manajemen keamanan informasi harus melibatkan seluruh pihak terkait. Standar ini membantu organisasi meningkatkan keamanan informasi dan mencegah pelanggaran data yang dapat membahayakan bisnis dan kredibilitas organisasi.

2.7 Tahapan Perencanaan SMKI

Untuk memastikan implementasi yang tepat, langkah pertama dalam penerapan SMKI adalah menentukan ruang lingkup dan batasan. Ruang lingkup mendefinisikan area dan aset yang dijangkau oleh sistem manajemen keamanan informasi. Hal ini mencakup aset fisik, informasi digital, proses, beserta personil yang bertanggung jawab dalam mengelola dan melindungi informasi. Di sisi lain, batasan mendeskripsikan area yang tidak termasuk dalam ruang lingkup, memberikan fokus yang jelas selama penerapan. Berikut ini akan diuraikan petunjuk untuk menyusun langkah-langkah sistem manajemen keamanan informasi (SMKI) yang difokuskan pada fase *Plan* (perencanaan).

2.7.1 Menentukan Ruang Lingkup dan Batasan

Untuk memastikan implementasi yang tepat, langkah pertama dalam penerapan SMKI adalah menentukan ruang lingkup dan batasan. Ruang lingkup mendefinisikan area dan aset yang dijangkau oleh sistem manajemen keamanan informasi. Hal ini mencakup aset fisik, informasi digital, proses, beserta personil yang bertanggung jawab dalam mengelola dan melindungi informasi. Di sisi lain, batasan mendeskripsikan area yang tidak termasuk dalam ruang lingkup, memberikan fokus yang jelas selama penerapan. Menetapkan cakupan SMKI

melibatkan penentuan cakupan penerapan SMKI yang akan diterapkan dalam struktur organisasi, apakah itu akan mencakup seluruh bagian organisasi atau hanya sebagian. Penetapan cakupan SMKI ini didasarkan pada:

1. Kebutuhan organisasi (proses, layanan, dan lokasi).
2. Aset yang dimiliki oleh organisasi.
3. Teknologi yang digunakan.

2.7.2 Menentukan Kebijakan Keamanan

Menetapkan kebijakan SMKI merupakan tekad manajemen untuk mendukung, memperkuat, menerapkan, menjalankan, mengawasi, mengevaluasi ulang, merawat, dan meningkatkan SMKI.

2.7.3 Penilaian Risiko

Penilaian Risiko (*Risk Assessment*) merupakan evaluasi risiko yang bermanfaat untuk memahami cara melakukan penilaian risiko sesuai dengan kebutuhan organisasi. Pelaksanaan penilaian risiko bergantung pada lingkup SMKI yang telah ditetapkan. Penilaian risiko bertujuan untuk mengetahui ancaman eksternal yang berpotensi mengganggu keamanan informasi organisasi dan potensi kerentanan yang mungkin dimiliki informasi dalam organisasi. Organisasi perlu menyadari dan mengambil langkah-langkah untuk memitigasi risiko kebocoran informasi, khususnya [16] :

1. Mengidentifikasi dan mendokumentasikan kriteria risiko keamanan informasi, yang meliputi:
   a. Kriteria penerimaan/termasi risiko (tingkat risiko misal tertentu dapat dipenuhi, namun pada tingkat di atasnya tidak dapat dipenuhi).
   b. Kriteria penilaian risiko keamanan informasi.
2. Memastikan bahwa penilaian risiko tinggi terhadap keamanan informasi akan memberikan hasil yang dapat diandalkan, valid, dan dapat dibandingkan.
3. Mengidentifikasi risiko keamanan informasi
   a. Menerapkan proses penilaian risiko pengelolaan informasi guna mengidentifikasi risiko terkait hilangnya informasi terkait

kerahasiaan/kerahasiaan (C), integritas (I), dan keterbukaan/ketersediaan (A) di domain SMKI.

b. Mengidentifikasi pemilik risiko.

4. Menganalisis risiko kebocoran informasi

a. Melakukan penilaian (menilai) terhadap potensi akibat yang dapat terjadi apabila risiko.

b. Menilai kemungkinan realistis terjadinya risiko yang teridentifikasi.

c. Menentukan tingkat risiko.

5. Mengevaluasi risiko keamanan informasi

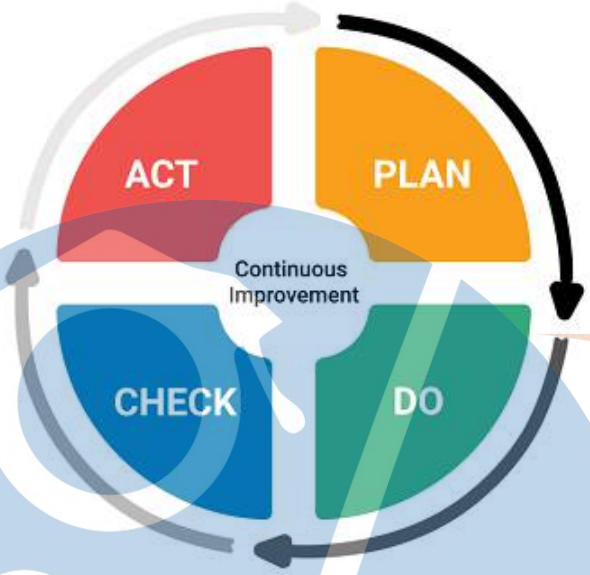
a. Membandingkan hasil analisis risiko dengan standar risiko yang telah ditetapkan.

b. Memprioritaskan risiko yang telah dianalisis untuk tindakan penanganan risiko.

c. Organisasi harus menyimpan informasi yang terdokumentasi tentang proses evaluasi risiko keamanan informasi.

2.7.4 Plan, Do, Check, Act (PDCA) Model

Untuk mendorong perbaikan berkelanjutan, model PDCA adalah siklus tindakan. Organisasi dapat menggunakannya sesuai dengan persyaratan ISO/IEC 27001 untuk mengimplementasikan Sistem Manajemen Keamanan Informasi (SMKI) (Fomin, 2008). Siklus PDCA terdiri dari empat bagian utama yang berurutan, yaitu:



Gambar 2. 3 Siklus PDCA (Langley et al., 2009)

1. ***Plan***

   Setelah pengujian selesai, langkah berikutnya adalah mengembangkan gagasan perbaikan masalah yang dirumuskan dengan jelas dan rinci, serta menetapkan tujuan dan sasaran yang ingin dicapai [16].

2. ***Do***

   Rencana yang dirancang diterapkan secara bertahap, mulai dari jumlah personel yang lebih kecil, dengan tugas dibagi secara merata sesuai dengan kemampuan dan kapasitas setiap anggota staf. Pengendalian harus dilakukan selama pelaksanaan rencana; ini berarti memastikan bahwa seluruh rencana dilaksanakan dengan sebaik mungkin agar sasaran dapat dicapai [16]. Langkah *Do* terdiri dari beberapa langkah, yaitu:

a. **Identifikasi Risiko**

   Identifikasi Risiko adalah untuk memahami sejauh mana dan mengidentifikasi jenis risiko yang mungkin dihadapi oleh sebuah organisasi jika informasi yang dimilikinya terancam atau terganggu keamanannya

sehingga mengakibatkan kegagalan dalam menjaga keamanan informasi. Langkah-langkah dalam proses identifikasi risiko meliputi:

1. Identifikasi Aset

   Mengidentifikasi aset yang sesuai dengan organisasi. Ini dapat dilakukan dengan menggunakan tabel berikut untuk mengidentifikasi aset:

Tabel 2. 1 Identifikasi Aset

Aset Organisasi		
No	Kategori Aset	Nama Aset
1.	*Hardware*	Komputer
		Laptop
		Sound System PC
		Printer
		Camera Digital
		Camera Logitech
		Proyektor
		Screen Proyektor
		Camera CCTV
2.	*Software*	Sistem Informasi
3.	Jaringan	WLAN
4.	Data	Data Anak Asuh
		Data Karyawan
		Data Pengajar
5.	Sumber Daya Manusia (SDM)	Karyawan
		Pengajar

2. Menghitung Nilai Aset

Menghitung nilai aset adalah penilaian data yang dimiliki oleh organisasi. Nilai aset yang dihitung hanya terdiri dari informasi yang termasuk dalam ruang lingkup SMKI yang telah didefinisikan. Kerahasiaan (*Confidentiality*), Keutuhan (*Integrity*), dan Ketersediaan (*Availability*) adalah tiga elemen keamanan informasi yang dapat digunakan untuk menghitung nilai aset [16]. Berikut ini adalah contoh penilaian aset berdasarkan Kerahasiaan.

a. **Kriteria Nilai *Confidentiality***

Tabel 2. 2 Contoh Penilaian Aset berdasarkan Kriteria Confidentiality

Kriteria *Confidentiality*	**Nilai *Confidentiality* (NC)**
Public	0
Internal use only	1
Private	2
Confidential	3
Secret	4

b. **Kriteria Nilai *Integrity***

Tabel 2. 3 Contoh Penilaian Aset berdasarkan Kriteria Integrity

Kriteria *Integrity*	**Nilai *Integrity* (NI)**
No Impact	0
Minor incident	1
General disturbance	2
Mayor disturbance	3

Unacceptable damage	4

c. **Kriteria Nilai *Availability***

Tabel 2. 4 Contoh Penilaian Aset berdasarkan Kriteria Availability

Kriteria *Availability*	**Nilai *Availability* (NV)**
No Availability	0
Office hours Availability	1
Strong Availability	2
High Availability	3

Nilai aset dapat dihitung dari ketiga tabel ini, yaitu:

Nilai Aset = NC + NI + NV

Keterangan:

NC = *Nilai Confidentiality*

NI = *Nilai Integrity*

NV = *Nilai Availability*

3. Mengidentifikasi Kelemahan, Ancaman dan Menilai Aset

a. Identifikasi Kelemahan

Tujuannya adalah agar organisasi memahami kelemahan sistem keamanan informasi. Kelemahan adalah kekurangan prosedur keamanan informasi, perencanaan, implementasi, atau kontrol internal, yang dapat menimbulkan atau menimbulkan ancaman.

b. Identifikasi Ancaman *(Threat Identification)*

Ancaman merupakan potensi yang timbul akibat kejadian yang tidak diinginkan yang berpotensi mengganggu kelancaran operasional suatu organisasi [16]. Identifikasi ancaman dilakukan untuk mengetahui potensi ancaman yang dapat mengganggu sistem di dalam organisasi. Berbagai macam contoh ancaman yang berasal dari berbagai sumber dapat ditemukan dalam tabel berikut.

Tabel 2. 5 Contoh Tabel Identifikasi Ancaman

No	Sumber Ancaman	Jenis Ancaman
1	Alam	Banjir, gempa bumi,, tornado, serangan petir
2	Lingkungan	Kegagalan sumber daya (*power failure*), polusi, bahan kimia berbahaya, kebocoran (cairan)
3	Manusia (*hacker*, Kriminal, Teroris)	(Hacking, penyusupan ke sistem, akses ilegal , Penyusupan ke sistem komputer, akses ilegal, *criminal computer*, *Blackmail*, penyerangan)

c. Menilai Aset

Untuk mengidentifikasi kelemahan, ancaman, dan menilai aset yang mungkin terkena dampak, digunakan tabel yang disebut tabel kemungkinan terjadi (*Probability of Occurrence*) [16].

Tabel 2. 6 Contoh Tabel Kemungkinan Terjadi

Hasil Rerata Probabilitas dan Nilai Ancaman				
No	**Kejadian**	**Jenis**	**Probabilitas**	**Perata Probabilitas**

1.	*Power failure* (Gangguan Sumber Daya)	*Vulnerable*	*Low*	0.1
2.	Hardware *Failure* (Gangguan Perangkat Keras)	*Vulnerable*	*Medium*	0.4
3.	*Fire* (Kebakaran)	*Threat*	*Low*	0.1
4.	*Virus Attack* (Serangan Virus)	*Threat*	*High*	0.7
5.	*Intruders* (Penyusup)	*Threat*	*Medium*	0.4
6.	*Data Corruption* (Kerusakan Data)	*Vulnerable*	*Medium*	0.4
7.	*Data Missing Recipient* (Kesalahan Pengiriman Data)	*Vulnerable*	*Low*	0.1

Tabel 2. 7 Contoh Tabel Kemungkinan Terjadi

Hasil Rerata Probabilitas dan Nilai Ancaman				
No	**Kejadian**	**Jenis**	**Probabilitas**	**Perata Probabilitas**
1.	*Lightning* (Gangguan Petir)	*Threat*	*Low*	0.1
2.	*Natural Disaster* (Bencana Alam)	*Threat*	*Low*	0.1
3.	*Unauthorized Access* (Akses	*Threat*	*Medium*	0.4

Hasil Rerata Probabilitas dan Nilai Ancaman				
No	**Kejadian**	**Jenis**	**Probabilitas**	**Perata Probabilitas**
	Ilegal)			

Nilai rerata probabilitas diperoleh dari kumpulan nilai yang dapat diukur:

Low : Nilai rerata probabilitas (0.1 – 0.3)

Medium : Nilai rerata probabilitas (0.4 – 0.6)

High : Nilai rerata probabilitas (0.7 – 1.0)

Untuk melakukan penilaian aset, dapat dihitung dengan rumus [16] :

Nilai Ancaman = ∑ PO x ∑ Ancaman

Keterangan :

∑ PO = Jumlah *Probability of Occurrence*

∑ Ancaman = Jumlah ancaman terhadap informasi

d. Melakukan analisis dampak bisnis untuk mengetahui bagaimana kegagalan akan berdampak pada organisasi.

b. Analisa dan Evaluasi Risiko

Setelah mengidentifikasi risiko pada langkah sebelumnya, langkah berikutnya adalah analisis dan evaluasi risiko. Tujuan dari tahapan ini adalah untuk memahami bagaimana risiko berdampak pada bisnis organisasi, tingkat risiko yang mungkin muncul, dan menentukan apakah risiko yang akan terjadi dapat diterima atau dapat dikelola untuk toleransinya. Analisis dan risiko terdiri dari beberapa langkah, seperti: Melakukan analisis dampak bisnis (*Business Impact Analysis)*, yang menunjukkan bagaimana proses bisnis berjalan di dalam organisasi secara konsisten. BIA memiliki skala di dalamnya, yang dapat disesuaikan sesuai dengan kebutuhan bisnis, seperti:

Tabel 2. 8 Skala Nilai BIA

Batas Toleransi Gangguan	Keterangan	Nilai BIA	Nilai Skala
< 1 Minggu	*Not critical*	0	0 - 20
1 Hari s/d 2 Hari	*Minor Critical*	1	21- 40
< 1 Hari	*Mayor Critical*	2	41 - 60
< 12 Jam	*High Critical*	3	61 - 80
< 1 Jam	*Very High Critica*	4	81 - 100

a. Mengidentifikasi level risiko

Level risiko merupakan tingkat risiko yang muncul ketika dikaitkan dengan dampak dan kemungkinan ancaman yang mungkin terjadi. Penentuan level risiko dapat dilakukan dengan menggunakan matriks level risiko yang sesuai dengan nilai-nilai probabilitas ancaman yang telah ditetapkan. Pengenalan level risiko dapat dijelaskan melalui matriks level risiko yang tercantum dalam tabel 2.7 [16].

Tabel 2. 9 Matriks Level Risiko

Probabilitas Ancaman	**Dampak Bisnis**				
	***Not critical* (20)**	***Low Critical* (40)**	***Medium Critical* (60)**	***High Critical* (80)**	***Very High Critical* (100)**
***Low* (0,1)**	*Low* 20 x 0,1 = 2	*Low* 40x0,1=4	*Low* 60 x 0,1 = 6	*Low* 80 x 0,1 = 8	*Low* 100 x 0,1 = 10

***Medium* (0,5)**	*Low* 20 x 0,5 = 10	*Medium* 40x0,5=20	*Medium* 60 x 0,5 = 30	*Medium* 80 x 0,5 = 40	*Medium* 100 x 0,5 = 50
***High* (1,0)**	*Medium* 20 x 1,0 = 20	*Medium* 40 x 1,0 = 40	*High* 60 x 1,0 = 60	*High* 80x1,0 = 80	*High* 100 x 1,0 = 100

b. Menentukan Risiko

Menilai kemungkinan risiko yang dapat diterima atau memerlukan tindakan pengelolaan risiko adalah proses untuk menentukan apakah risiko tersebut dapat diterima atau masih memerlukan tindakan pengelolaan risiko berdasarkan standar penerimaan risiko. Untuk menentukan tingkat risiko yang tepat, nilai risiko harus dihitung untuk menentukan posisi level dari setiap aset dengan menggunakan rumus berikut:

Nilai Risiko (Risk Value) = NA x BIA x NT

Keterangan:

NA : Nilai Aset

BIA : Analisa Dampak Bisnis (*Business Impact Analysis*)

NT : Nilai Ancaman

3. Check

Memeriksa atau melakukan penelitian yang berkaitan dengan penetapan untuk memastikan bahwa pelaksanaannya berjalan sesuai rencana dan mengawasi kemajuan perbaikan yang direncanakan [16].

4. Act

Didasarkan pada hasil analisis sebelumnya, penyesuaian dilakukan jika dianggap perlu. Menyesuaikan prosedur baru untuk mencegah masalah yang sama muncul lagi atau menetapkan tujuan baru untuk perbaikan. Ada kemungkinan bahwa model PDCA *(Plan, Do, Check, Act*) adalah model yang dapat terus membantu memperbaiki sistem [16].

1. Tahap *Plan*, dilakukan penetapan pada sasaran dan target ditetapkan
2. Tahap *Do*, risiko diidentifikasi (dengan mengidentifikasi aset, menghitung nilai aset, mengidentifikasi kelemahan, ancaman, dan menilai aset, dan melakukan analisis dampak pada bisnis), dan analisis dan evaluasi risiko.
3. Tahap *Check*, apakah pelaksanaan telah sesuai dengan rencana.
4. Tahap *Act*, melakukan penyesuaian tambahan berdasarkan celah dan saran.

Penelitian ini menggunakan model PDCA pada tahap *Plan* mendefinisikan ruang lingkup dan perencanaan kebijakan SMKI.

2.8 Manajemen Risiko

Risiko adalah situasi yang belum tentu akan terjadi atau dihadapi oleh manusia dalam setiap tindakannya. Risiko juga merupakan ketidakpastian tentang apa yang akan terjadi di masa depan. Risiko merupakan potensi terjadinya kerugian yang timbul saat ancaman mengungkapkan kelemahan. Melakukan analisis risiko untuk menilai kerentanan dan ancaman yang mungkin terjadi pada aset informasi tersebut. Mengukur risiko keamanan informasi merupakan tugas yang kompleks dalam sebuah sistem informasi. Evaluasi risiko dapat dilakukan dengan dua pendekatan, yaitu kualitatif dan kuantitatif. Dalam pendekatan kuantitatif, terdapat proses penilaian dari setiap aset secara terperinci. Menentukan nilai aset seperti informasi atau *database* merupakan hal yang transparan karena proses penilaian tersebut melibatkan elemen-elemen yang harus diestimasi [13].

Di sisi lain, pendekatan kualitatif menggunakan metode wawancara atau kuesioner untuk mengumpulkan fakta melalui perkiraan statistik dengan hasil tingkat rendah, sedang, dan tinggi sehingga sulit untuk menghitung kerugian finansial hanya berdasarkan asumsi. Pendekatan kualitatif cenderung didominasi oleh pengukuran subjektif, sementara pendekatan kuantitatif dapat menghilangkan unsur subjektif tersebut.

Pendekatan kuantitatif lebih objektif dibandingkan dengan pendekatan kualitatif. Manajemen risiko merupakan bagian integral dari manajemen sistem

informasi yang bertujuan untuk mengevaluasi ancaman dan kerentanan sistem informasi serta aset yang dimiliki. Manajemen risiko juga dapat mengurangi risiko seperti proses bisnis yang tidak optimal, pemborosan anggaran, dan penurunan reputasi organisasi. Mengurangi risiko bukan berarti menghilangkannya, tetapi menurunkan risiko ke tingkat yang dapat diterima oleh organisasi. Untuk memastikan keamanan informasi, diperlukan analisis risiko yang efektif, definisi ancaman, dan dampak yang ditimbulkan oleh risiko tersebut [14].

Dengan melakukan analisis dan identifikasi risiko, organisasi dapat mengembangkan strategi yang tepat untuk keamanan informasi dan mengurangi kemungkinan munculnya risiko yang dapat berdampak pada aset penting atau rahasia yang tidak terlindungi. Fokus pada penilaian aset yang dimiliki merupakan kunci keberlangsungan organisasi. Tujuan dari analisis risiko adalah untuk memberikan gambaran tentang kemungkinan munculnya ancaman sehingga organisasi dapat merancang strategi dan langkah-langkah untuk mengurangi dan mengevaluasi risiko. Hasil analisis risiko dapat direpresentasikan dalam bentuk matriks risiko.

2.8.1 Pentingnya Manajemen Risiko

Manajemen risiko adalah bidang studi yang membahas cara lembaga atau organisasi mengenali masalah dengan pendekatan manajemen yang komprehensif dan terstruktur [14].

Tujuan dari manajemen risiko adalah untuk memberikan pemahaman kepada organisasi mengenai :

a. Evaluasi terhadap tingkat dampak atau risiko yang mungkin terjadi jika terjadi kegagalan dalam keamanan informasi di dalam organisasi.
b. Identifikasi ancaman (*Threat*) terhadap informasi organisasi beserta kelemahan (*Vulnerability*) yang dimiliki oleh informasi organisasi yang dapat mengakibatkan kegagalan dalam keamanan informasi.
c. Strategi penanganan risiko terhadap kegagalan keamanan informasi dapat dilakukan dengan cara:
    1. Menerima risiko yang mungkin terjadi (*risk acceptance*).

2. Mengurangi risiko yang mungkin terjadi (*risk reducement*).
3. Menghindari atau memindahkan risiko kepada pihak lain (*risk transfer*).
4. Penentuan kontrol keamanan yang diperlukan oleh organisasi untuk memenuhi standar manajemen risiko yang telah ditetapkan.

Tanpa adanya manajemen risiko, organisasi tidak akan mampu menentukan kontrol keamanan yang diperlukan dalam penerapan SMKI. Sementara kontrol keamanan sendiri merupakan aspek yang sangat vital dalam perencanaan SMKI.

Gambar 2. 4 Analisis Risiko

2.8.2 Risiko Teknologi Informasi

Ketika merancang sistem manajemen keamanan informasi, organisasi harus mempertimbangkan isu-isu yang relevan dari dalam dan luar organisasi. Ini penting untuk mengidentifikasi pihak-pihak yang terlibat dalam sistem manajemen keamanan informasi dan persyaratan yang harus dipenuhi oleh mereka. Selain itu, organisasi juga perlu mengenali risiko dan peluang yang perlu ditangani untuk memastikan sistem manajemen keamanan informasi mencapai manfaat yang diinginkan, mencegah dampak yang tidak diinginkan, dan mencapai peningkatan yang berkelanjutan.

Dalam perencanaan sistem manajemen keamanan informasi, organisasi harus menetapkan langkah-langkah untuk mengelola risiko dan peluang yang ada.

Selain itu, organisasi juga harus merencanakan bagaimana cara mengintegrasikan dan menerapkan langkah-langkah tersebut ke dalam proses sistem manajemen keamanan informasi, serta mengevaluasi keefektifan dari langkah-langkah yang telah diambil [14].

2.8.3 Pengelolaan Risiko

Saat merencanakan Sistem Manajemen Keamanan Informasi (SMKI), organisasi perlu mempertimbangkan aspek yang tercakup dalam memahami struktur organisasi dan lingkungannya serta kebutuhan yang tercakup dalam memahami kebutuhan dan harapan dari pihak yang berkepentingan, serta mengidentifikasi risiko dan peluang yang perlu diatasi untuk:

a. Memastikan SMKI dapat mencapai manfaat yang diinginkan.
b. Mencegah atau mengurangi dampak yang tidak diinginkan.
c. Mencapai peningkatan keamanan informasi yang berkelanjutan [15].

Pada proses pengelolaan manajemen risiko keamanan informasi terdiri dari tiga langkah utama, yaitu identifikasi risiko, analisis risiko, dan evaluasi risiko. proses pengelolaan risiko mencakup beberapa tahapan penting:

1. Identifikasi Risiko

   Identifikasi risiko adalah proses mengidentifikasi dan mendokumentasikan risiko yang dapat mempengaruhi keamanan informasi organisasi.

   Langkah-langkah:

   1. Mengidentifikasi Aset Informasi: Menentukan dan mencatat semua aset informasi yang dimiliki, seperti data pribadi anak yatim, data donatur, sistem manajemen informasi, perangkat keras, perangkat lunak, dan dokumentasi fisik.
   2. Mengidentifikasi Ancaman: Mengidentifikasi potensi ancaman dari luar (misalnya, serangan siber, bencana alam) maupun dari dalam (misalnya, kesalahan manusia, kebocoran informasi).
   3. Mengidentifikasi Kerentanan: Menilai kelemahan dalam sistem keamanan informasi yang dapat dieksploitasi oleh ancaman, seperti

perangkat lunak yang tidak diperbarui, kebijakan keamanan yang lemah, atau kurangnya pelatihan bagi karyawan.

2. Analisis Risiko

Analisis risiko adalah proses menilai risiko yang telah diidentifikasi untuk memahami dampaknya terhadap organisasi dan menentukan tingkat keparahan risiko tersebut.

Langkah-langkah:

1. Menilai Dampak : Menilai potensi dampak dari setiap risiko terhadap organisasi. Dampak dapat diukur dari berbagai aspek, seperti kerugian finansial, kerusakan reputasi, gangguan operasional, dan hilangnya data.
2. Menilai Kemungkinan: Menentukan seberapa besar kemungkinan terjadinya setiap risiko berdasarkan data historis, pola serangan yang telah terjadi, dan analisis *trend*.
3. Menentukan Tingkat Risiko: Menggabungkan penilaian dampak dan kemungkinan untuk menentukan tingkat risiko (misalnya, rendah, sedang, tinggi). Hal ini biasanya dilakukan dengan menggunakan matriks risiko.

3. Evaluasi Risiko

Evaluasi risiko adalah proses menilai apakah hasil analisis risiko sudah sesuai dengan teori dan praktik terbaik, serta menentukan prioritas tindakan untuk menangani risiko tersebut.

Langkah-langkah:

1. Mengecek Kesesuaian dengan Teori: Memastikan bahwa hasil analisis risiko sesuai dengan metodologi yang telah ditetapkan dan teori manajemen risiko yang berlaku. Ini melibatkan peninjauan kembali setiap penilaian dampak dan kemungkinan.
2. Validasi dengan Data dan Skenario Nyata: Menggunakan data aktual dan skenario yang mungkin terjadi untuk memvalidasi hasil analisis risiko.

3. Membuat Daftar Prioritas Penanganan Risiko: Menetapkan prioritas penanganan risiko berdasarkan tingkat risiko yang telah diidentifikasi. Risiko dengan dampak tinggi dan kemungkinan tinggi menjadi prioritas utama.
4. Merencanakan Tindakan Pengendalian: Menentukan tindakan pengendalian yang perlu diambil untuk mengurangi atau mengelola risiko. Tindakan ini bisa berupa pencegahan, deteksi, respon, atau pemulihan.
5. Menyusun Rencana Penanganan Risiko: Membuat rencana penanganan risiko yang mencakup tindakan pengendalian, sumber daya yang diperlukan, dan jadwal pelaksanaan.

Dengan menerapkan pengelolaan risiko yang efektif, Pondok Yatim Dhuafa dapat melindungi aset informasinya dari berbagai ancaman, memastikan kerahasiaan, integritas, dan ketersediaan informasi, serta mematuhi peraturan dan standar yang berlaku. Langkah-langkah ini membantu organisasi dalam mencapai tujuannya dengan lebih aman dan terjamin.

2.9 Penelitian Terkait

Tabel 2. 10 Penelitian Terkait

No	Nama dan Tahun	Judul	Topik	Subjek	Hasil
1	Yusuf Baharudin Nizar (2021)	Perencanaan Sistem Manajemen Keamanan Informasi Berdasarkan Standar ISO/IEC 27001:2013	Sistem Manajemen Keamanan Informasi	PT Angkasa Pura 1	Menghasilkan dokumen manajemen risiko yang berhubungan dengan keamanan informasi, seperti mengevaluasi risiko, mengidentifikasi risiko, menganalisis dan mengevaluasi risiko,

		Pada PT Angkasa Pura 1 (PERSERO) Surabaya			serta mengidentifikasi dan mengevaluasi penanganan risiko yang terkait dengan PT Angkasa Pura 1 (Persero) Surabaya. Dokumen Standar Prosedur Operasional (SOP) mencakup dokumen kebijakan, petunjuk kerja, dan prosedur yang terkait dengan penetapan kontrol objektif dan keamanan dari manajemen risiko terkait keamanan informasi[8].
2	Wilda Ayu Pratiwi (2019)	Perencanaan Sistem Manajemen Keamanan Informasi Berdasarkan Standar ISO 27001:2013 Pada KOMINFO Jawa Barat	Sistem Manajemen Keamanan Informasi	PT Kominfo	Dokumen pengelolaan manajemen risiko telah berhasil disusun dengan tahapan identifikasi risiko, penilaian risiko dan respon risiko pada setiap aset informasi. Pengendalian keamanan pada dokumen ini dibagi menjadi 3 kategori,

					yaitu kategori manajemen dengan 2 pengendalian keamanan, kategori teknis dengan 9 pengendalian keamanan, dan kategori operasional dengan 3 pengendalian keamanan. Dokumen *Standard Operating Procedure* (SOP) juga telah berhasil disusun sesuai kebutuhan, antara lain dokumen kebijakan, SOP, instruksi kerja dan formulir. Dokumen persyaratan teknis terdiri dari dokumen kebijakan, SOP, instruksi kerja, dan formulir yang mendukung keamanan informasi dan penerapan SMKI.[9].
3	Nurul Octariza	Analisis Sistem	Sistem Manajemen	PT. Jasa Marga	Dari hasil penelitian ini, ISO/IEC 27001

	Fadhylah, 2019	Manajemen Keamanan Informasi Menggunakan Standar ISO/IEC 27001 dan ISO/IEC 27002 Pada Kantor Pusat PT. Jasa Marga	Keamanan Informasi		memberikan prioritas pada standarisasi kebijakan terkait PT Jasa Marga dan manajemen risiko karena belum mengimplementasikan kebijakan IT. Hal ini terutama terkait dengan pengelolaan aset dan manajemen operasional yang disesuaikan dengan kebutuhan PT Jasa Marga. [10]

2.9.1 Penelitian Yusuf Baharudin Nizar (2021)

Tujuan dari penelitian ini adalah untuk menciptakan dokumen kontrol yang bersifat objektif dan keamanan terkait manajemen risiko keamanan informasi, yang mencakup: evaluasi risiko, identifikasi risiko, analisis dan penilaian risiko, serta penanganan risiko di PT Angkasa Pura 1 (Persero) Surabaya. Dokumen Standar Operasional Prosedur (SOP) mencakup: kebijakan dokumen, instruksi kerja, dan catatan kerja yang sesuai dengan kontrol objektif dan keamanan dari manajemen risiko terkait keamanan informasi [8].

2.9.2 Penelitian Wilda Ayu Pratiwi (2019)

Penelitian ini bertujuan untuk menghasilkan tahap penyusunan dokumen. Dokumen pengelolaan manajemen risiko telah berhasil disusun dengan tahapan identifikasi risiko, penilaian risiko dan respon risiko pada

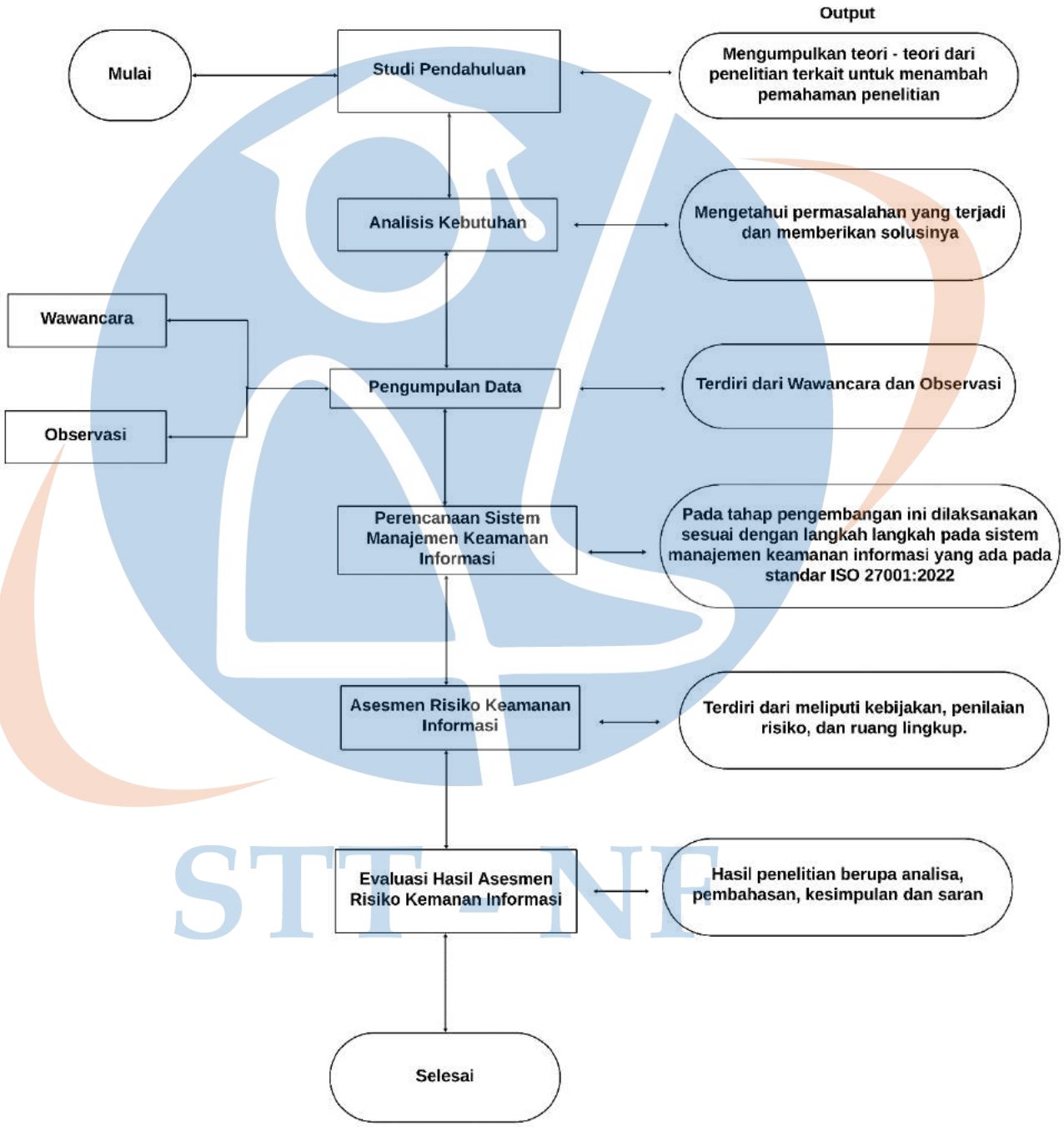
setiap aset informasi. Pengendalian keamanan pada dokumen ini dibagi menjadi 3 kategori, yaitu kategori manajemen dengan 2 pengendalian keamanan, kategori teknis dengan 9 pengendalian keamanan, dan kategori operasional dengan 3 pengendalian keamanan. Dokumen *Standard Operating Procedure* (SOP) juga telah berhasil disusun sesuai kebutuhan, antara lain dokumen kebijakan, SOP, instruksi kerja dan formulir. Dokumen persyaratan teknis terdiri dari dokumen kebijakan, SOP, instruksi kerja, dan formulir yang mendukung keamanan informasi dan penerapan SMKI [9].

2.9.3 Penelitian Nurul Octariza Fadhylah (2019)

Hasil penelitian ini, ISO/IEC 27001 memberikan prioritas pada standarisasi kebijakan terkait PT Jasa Marga dan manajemen risiko karena belum mengimplementasikan kebijakan IT. Hal ini terutama terkait dengan pengelolaan aset dan manajemen operasional yang disesuaikan dengan kebutuhan PT Jasa Marga [10].

BAB III
METODE PENELITIAN

3.1 Tahap Penelitian



Gambar 3. 1 Tahapan Penelitian

3.1.1 Studi Pendahuluan

Untuk membantu menyelesaikan tugas akhir pada tahap pengembangan hingga tahap akhir, penelitian literatur perlu dilakukan. Ini dilakukan dengan cara mempelajari, memahami, dan mencari referensi yang relevan melalui jurnal ilmiah, *e-book*, artikel, tesis, atau sumber lain yang terkait dengan topik penelitian.

3.1.2 Analisis Kebutuhan

Tujuan dari identifikasi masalah PYD Thursina adalah untuk mengetahui masalah saat ini melalui hasil wawancara dan observasi. Ini dimulai dengan masukan mengenai masalah saat ini, setelah pengumpulan data dan referensi tentang subjek yang dibahas dalam penelitian ini. Setelah mengetahui permasalahan pada PYD Thursina, selanjutnya akan menganalisis masalah dalam metode penelitian sebagai proses identifikasi, pemahaman, dan pemecahan masalah yang menjadi fokus penelitian. Dengan tujuan dari analisis masalah yaitu untuk mencari pemahaman yang lebih mendalam tentang masalah-masalah yang akan diteliti, sehingga langkah-langkah yang tepat dapat diambil untuk memecahkan masalah tersebut.

3.1.3 Pengumpulan Data

Pada tahap ini merupakan penjelasan dalam pengumpulan data kualitatif dengan langkah krusial dalam metode penelitian yang bertujuan untuk mendapatkan pemahaman mendalam tentang fenomena yang diteliti. Pendekatan ini memungkinkan peneliti untuk mengeksplorasi perspektif, pengalaman, dan makna yang diberikan oleh individu atau kelompok terkait topik penelitian.

3.1.4 Perencanaan Sistem Manajemen Keamanan Informasi

Pada tahapan ini, setelah adanya kebutuhan yang sudah terpenuhi maka langkah selanjutnya melakukan penyusunan pada perencanaan dokumen SMKI berdasarkan ISO/IEC 27001:2022.

3.1.5 Pengelolaan Risiko Keamanan Informasi

Manajemen risiko keamanan informasi memegang peranan penting dalam proses manajemen risiko dengan tujuan untuk mengenali, menganalisis, dan mengevaluasi ancaman serta kerentanan yang dapat membahayakan keamanan informasi. Berikut ini merupakan penjelasan mengenai langkah-langkah dalam pengelolaan risiko keamanan informasi:

1. Pengenalan Risiko Keamanan Informasi

   Pengenalan risiko merupakan langkah awal dalam pengelolaan risiko keamanan informasi. Pada tahap ini, organisasi berupaya untuk mengidentifikasi ancaman dan kerentanan yang dapat membahayakan aset informasi mereka. Beberapa kegiatan yang dilakukan pada tahap ini meliputi:

   a. Pengenalan aset informasi: Menentukan dan mencatat semua aset informasi yang dimiliki oleh organisasi, seperti data sensitif, sistem informasi, perangkat keras, dan perangkat lunak. Berikut kategori aset informasi.
   b. Pengenalan ancaman: Mengidentifikasi potensi ancaman dari luar (seperti serangan siber, *malware*, bencana alam) maupun dari dalam (seperti kesalahan manusia, kebocoran informasi oleh karyawan).

2. Analisis Risiko Keamanan Informasi

   Setelah risiko diidentifikasi, langkah berikutnya adalah menganalisis risiko tersebut untuk memahami dampaknya terhadap organisasi. Kegiatan dalam tahap ini meliputi:

   a. Menilai dampak : Menilai potensi dampak dari setiap risiko terhadap organisasi, seperti kerugian finansial, kerusakan reputasi, gangguan operasional, dan kehilangan data.
   b. Menilai kemungkinan : Menentukan seberapa besar kemungkinan terjadinya setiap risiko berdasarkan data *historis*, pola serangan, dan analisis *trend*.
   c. Penetapan level risiko : Menggabungkan evaluasi dampak dan kemungkinan untuk menentukan level risiko (rendah, sedang,

tinggi) dengan menggunakan matriks risiko atau alat penilaian risiko lainnya.

3. Evaluasi Risiko Keamanan Informasi

   Evaluasi risiko adalah tahap di mana organisasi menetapkan prioritas tindakan berdasarkan analisis risiko yang telah dilakukan. Kegiatan pada tahap ini meliputi:

   a. Perbandingan risiko: Membandingkan risiko yang telah diidentifikasi dan dianalisis dengan kriteria risiko yang telah ditetapkan oleh organisasi untuk menentukan tindakan yang perlu diambil
   b. Penetapan tindakan pengendalian: Menentukan langkah-langkah untuk mengurangi atau mengelola risiko, seperti pencegahan, deteksi, respon, atau pemulihan.
   c. Penetapan prioritas: Menetapkan prioritas dalam penanganan risiko berdasarkan tingkat risiko dan sumber daya yang tersedia, dengan risiko tinggi menjadi prioritas utama.
   d. Dokumentasi dan pelaporan: Mendokumentasikan hasil evaluasi risiko dan menyusun laporan untuk disampaikan kepada manajemen senior atau pihak terkait.

3.1.6 Evaluasi Hasil Perencanaan Sistem Manajemen Keamanan Informasi

Pada bagian ini, setelah perancangan selesai, dokumen evaluasi hasil diskusi penelitian dilakukan melalui proses Plan pada proses PDCA sesuai dengan metode pelaksanaan yang direncanakan.

3.1.7 Kesimpulan dan Saran

Kesimpulan pada penelitian ini disampaikan sebagai acuan untuk penelitian selanjutnya.

3.2 Rencana Penelitian

3.2.1 Jenis Penelitian

Jenis penelitian yang digunakan pada penelitian ini adalah Penelitian Tindakan atau *Action Research*. Metode ini berfokus pada tindakan praktis untuk memecahkan masalah yang sedang dihadapi.

3.2.2 Metode Analisis

Metode analisis data kualitatif melibatkan proses yang sistematis untuk mengidentifikasi tema, pola, dan makna dari data non-numerik. Dalam konteks perencanaan Sistem Manajemen Keamanan Informasi (SMKI) berbasis ISO/IEC 27001:2022 di Pondok Yatim Dhuafa Thursina Bogor, analisis data kualitatif dapat memberikan wawasan mendalam tentang kondisi keamanan informasi dan tindakan yang diperlukan untuk perbaikan. Jenis data yang dikumpulkan dalam penelitian ini berupa:

1. Wawancara: Transkip wawancara dengan narasumber yang bersangkutan
2. Observasi: Catatan lapangan yang mencakup pengamatan terhadap praktik keamanan informasi di pondok.
3. Dokumen: Analisis dokumen kebijakan keamanan informasi dan catatan insiden keamanan.

Jenis data ini akan memberikan pemahaman yang lebih luas dan mendalam mengenai proses, dan manfaat dari penerapan SMKI, melalui pengalaman dan perspektif para pengelola serta para pihak lainnya di Pondok Yatim Dhuafa Thursina Bogor. Untuk mendapatkan pemahaman yang berharga tentang subjek dan objek yang sedang diteliti, wawancara dapat menjadi *tools* yang cukup baik untuk mengumpulkan data kualitatif yang mendalam.

3.2.3 Metode Pengumpulan Data

Dalam penelitian ini, penulis menggunakan teknik berikut untuk mengumpulkan informasi:

1. Wawancara

   Wawancara dalah teknik pengumpulan data kualitatif yang melibatkan interaksi langsung antara peneliti dan partisipan untuk memperoleh informasi yang mendalam tentang subjek penelitian. Wawancara dapat dilakukan secara tatap muka, melalui telepon, atau secara virtual menggunakan platform digital. Jenis wawancara yang digunakan pada penelitian ini dengan wawancara tidak struktur, dimana tidak ada daftar pertanyaan yang telah disiapkan sebelumnya. Peneliti lebih mengandalkan percakapan yang alami untuk mengumpulkan data.

2. Observasi

   Observasi adalah metode pengumpulan data di mana peneliti mengamati dan mencatat perilaku, kejadian, atau kondisi dalam lingkungan alami. Observasi dapat bersifat partisipatif atau non-partisipatif, tergantung pada sejauh mana peneliti terlibat dalam kegiatan yang diamati. Metode ini dapat dilakukan dalam berbagai bentuk, mulai dari penelitian ilmiah hingga pengamatan lapangan dalam studi pasar atau survei sosial. Dengan menggunakan teknik observasi, peneliti dapat memperoleh data yang akurat dan mendasar tentang subjek tanpa mengubah lingkungan atau perilaku yang diamati. Jenis observasi yang digunakan pada penelitian ini adalah non-partisipatif, dimana eneliti mengamati kejadian atau perilaku tanpa berpartisipasi dalam aktivitas tersebut.

3.2.4 Metode Pengujian

Penelitian ini memanfaatkan teknik pengujian UAT (*User Acceptance Test*). Pendekatan ini dipakai untuk menunjukkan bahwa sebuah alat sudah memenuhi kriteria yang ditetapkan. UAT dilakukan dengan melakukan interaksi dengan pihak terkait untuk menilai hasil dari penyusunan dokumen.

3.2.5 Lingkungan Pengembangan

a. Lokasi Penelitian

Lokasi penelitian ini dilakukan di Pondok Yatim dan Dhuafa Thursina yang berlokasi di Jl. Pirus, Kp. Baru Tegal RT 002 RW 008, Desa Cibeureum, Kecamatan Cisarua, Kabupaten Bogor, Provinsi Jawa Barat, Kode Pos 16750.

b. Alat Penelitian

Tabel 3. 1 Alat Penelitian (Pribadi)

No.	Alat	Keterangan
1.	Hp Laptop 14-cf2xxx	Hp Laptop 14-cf2xxx dengan spesifikasi sebagai berikut : • *Operating System*: Windows 10 Home 64-bit • *Processor*: Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz (8 CPUs), ~2.1GHz • *Memory*: 8192MB RAM • Monitor : 14 Led • Mouse : X - Craft Electro
2.	Lucidchart	Platform yang digunakan untuk membuat bagan dalam tahap penelitian
3.	Microsoft Office	Platform yang digunakan untuk mengolah dan menghasilkan data dalam penyusunan penulisan
4.	Google Chrome & Google Scholar	Platform yang digunakan untuk mengakses informasi, memperluas pemahaman & wawasan selama proses penelitian berlangsung.

BAB IV
HASIL DAN PEMBAHASAN

Berikut adalah hasil dari proses pembuatan Perencanaan Sistem Manajemen Keamanan Informasi berdasarkan Standar ISO 27001:2022 di Pondok Yatim Dhuafa Thursina Bogor, mulai dari tahap awal hingga tahap akhir.`

4.1 Studi Pendahuluan

Studi pendahuluan dilakukan untuk mendukung penyelesaian tugas akhir dari tahap pengembangan hingga tahap akhir dengan merujuk pada sumber-sumber yang relevan. Sumber-sumber ini termasuk buku-buku di perpustakaan dan jurnal-jurnal terkait topik penelitian, sehingga dapat memberikan dukungan dan menjawab tujuan serta masalah terkait topik tersebut. Masalah yang dihadapi oleh PYD Thursina dan tujuan yang ingin dicapai adalah implementasi sistem manajemen keamanan informasi di PYD Thursina. Metode studi pendahuluan yang digunakan dalam penyusunan laporan ini melibatkan penyusunan pengelolaan risiko keamanan informasi dan konsep pengelolaan risiko keamanan informasi.

4.2 Analisis Kebutuhan

4.2.1 Wawancara

Wawancara yang dilakukan pada penelitian ini dengan Bapak M. Ikbar Muhyi Maulani, S.Kom, M.Pd selaku Pimpinan Pondok Yatim Dhuafa Thursina Bogor pada PYDT mengenai kebutuhan yang akan dilakukan dalam pelaksanaan tugas akhir. Wawancara bertujuan untuk mengetahui informasi, dan kelemahan apa yang didapat serta nantinya dapat memberikan solusi bagi permasalahan yang ada.

Tabel 4 1 Hasil Wawancara

Hasil Wawancara		
P	:	Kepada Pak Ikbar selaku Pimpinan PYDT, ingin bertanya pak. Apakah pondok yatim dhuafa ini sudah menerapkan sistem manajemen keamanan informasi? Jika ya, sejak kapan?

N	:	Untuk sistem manajemen keamanan informasi, kami belum ada sistem keamanan perihal yang dimaksud dalam penelitian ini. Jika dalam penelitian ini dapat membantu dalam membentuk sistem keamanan informasi, Insha Allah kita bisa *aware* ataupun bisa menerima masukan-masukan dan apa yang harus dilakukan dalam suatu lembaga ketika ada teknologi yang harus dijaga pada keamanan informasi.
P	:	Selanjutnya, Apakah selama belum ada keamanan sistem informasi ada insiden atau pernah terjadi pada sistem informasi di pondok yatim dhuafa? Jika ya, bagaimana penanganannya?
N	:	Selama ini, *Alhamdulilah* belum ada kendala atau pernah terjadi seperti kehilangan data, ke *hack* atau kesalahan data.
P	:	Jika berkenan dan boleh usul, untuk dalam sistem informasi pada PYDT ini dapat menerapkan manajemen keamanan informasi yang sesuai dengan ISO/IEC 27001 ?
N	:	Sebelumnya dari saya sangat berterima kasih ya, kalau dalam penelitian ini mau bantu dalam menerapkan sistem keamanan informasi pada lembaga ini, karena kita belum ke arah sana. Dan harapannya bisa menerapkan dalam menjaga sistem keamanan informasi yang ada di pondok ini.
P	:	Dalam penyusunan awal dalam SMKI, sekiranya apa yang dibutuhkan dari PYDT khususnya pada sistem informasi ini?
N	:	Pada awal terkait penerapan ISO 27001 dalam pengelolaan aset serta penilaian risiko yang belum terstruktur dan terarah.

4.2.2 Hasil Wawancara

Pada sesi wawancara dalam subbab 4.2.1, Pondok Yatim Dhuafa Thursina saat ini belum menerapkan SMKI yang berstandar ISO 27001. Peneliti memberikan usul untuk dapat menerapkan SMKI yang berstandar ISO 27001 dan saat ini dibutuhkannya pengelolaan risiko aset informasinya dengan cara yang sistematis

dan terstruktur. Dalam hal penyusunan perencanaan SMKI, peneliti membutuhkan lembaga PYDT untuk menentukan ruang lingkup sesuai dengan kebutuhan dalam menentukan proses dan perencanaan di PYDT terkait keamanan informasi, dengan fokus pada pengendalian informasi.

4.2.3 Observasi

Observasi ini dilakukan secara tidak langsung pada PYDT melibatkan pengumpulan data tanpa interaksi langsung dengan objek yang diamati. Metode ini disebut sebagai observasi non-partisipatif atau observasi pasif. Berikut adalah penjelasan tentang bagaimana observasi tidak langsung dapat dilakukan di PYD Thursina :

1. Pengamatan Lingkungan.
   Observasi ini bisa mencakup cara perangkat keras disimpan dan dilindungi, serta bagaimana akses ke informasi sensitif dikelola.
2. Analisis Dokumen.
   Peneliti mengumpulkan dan menganalisis dokumen-dokumen internal yang tersedia, seperti dokumen anak asuh, karyawan, dan sistem keamanannya.

4.3 Perencanaan Sistem Manajemen Keamanan Informasi

4.3.1 Menentukan Ruang Lingkup SMKI

Proses dan kegiatan perencanaan di PYDT membahas keamanan informasi, dengan fokus pada pengendalian informasi. Oleh karena itu, untuk mematuhi standar ISO 27001:2022, perlindungan informasi harus dimaksimalkan. SMKI organisasi digunakan untuk seluruh operasinya, yaitu PYDT memiliki karakteristik unik yang mencakup profil, visi, dan misi yang ingin dipelajari lebih lanjut. Lokasi PYDT digunakan untuk memahami struktur organisasi dan tugas-tugas yang ada. Aset-aset yang dimiliki oleh PYDT, termasuk aset informasi dan lainnya, diidentifikasi untuk menentukan jenis aset yang ada. Penggunaan teknologi di PYDT bertujuan untuk mengidentifikasi teknologi yang digunakan dalam aktivitas sehari-hari, seperti server, kabel LAN, dan sebagainya.

4.3.2 Menentukan Kebijakan SMKI

Perencanaan Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan standar ISO/IEC 27001:2022 menyediakan serangkaian proses untuk operasional keamanan teknologi informasi yang menjadi kebijakan dan dasar pelaksanaan SMKI. Bersama dengan ISO/IEC 27002:2022, yang berfokus pada keamanan dan kontrol akses informasi, standar ini memungkinkan penerapan langkah-langkah keamanan yang tepat. Untuk memastikan kelancaran proses di PYDT, diperlukan perlindungan aset organisasi melalui implementasi SMKI yang efektif. Kebutuhan PYDT selalu berubah seiring perkembangan, sehingga PYDT harus mampu mengembangkan dan memelihara SMKI yang sesuai dengan kebutuhan yang dinamis. Berikut adalah panduan dan tujuan penerapan SMKI sesuai dengan kebijakan dan kontrol akses keamanan informasi yang memungkinkan bisnis untuk menerapkan langkah-langkah keamanan yang tepat.

1. Tujuan

   Tujuan kebijakan keamanan informasi dan kontrol akses adalah bagian dari SMKI yang harus diikuti oleh semua karyawan dan pengajar di PYDT. Kebijakan ini bertujuan untuk melindungi:

   a. Integritas: Menjaga keutuhan dan kualitas informasi agar tetap aman dan benar.
   b. Kerahasiaan: Memastikan informasi hanya dapat diakses oleh pihak yang berwenang.
   c. Ketersediaan: Menjamin informasi dan teknologi informasi siap digunakan kapan pun dibutuhkan.

Kebijakan keamanan informasi digunakan untuk melindungi informasi organisasi dan teknologi informasi di PYDT. Kontrol akses keamanan informasi berfokus pada aspek teknis, pemeliharaan aset, dan tingkat keamanan, khususnya dalam kondisi fisik untuk pemeliharaan di PYDT.

2. Kebijakan Keamanan Informasi

   Untuk menerapkan perlindungan aset informasi secara tepat, terlepas dari nilai ancaman dan kerentanan yang dapat terjadi, Ketua Pimpinan PYDT akan memastikan seluruh sistem berfungsi dengan baik. Tujuan kebijakan

ini adalah membangun SMKI sesuai dengan standar ISO/IEC 27001:2022 di PYDT, agar dapat mencegah akses yang tidak sah, transfer data, perubahan data, kerusakan data, dan pencurian aset informasi. Pimpinan PYDT bertujuan mengajak seluruh pegawai untuk mematuhi kebijakan, kontrol, dan pedoman yang ada dengan mengadakan pelatihan keamanan informasi. Ketua Pimpinan PYDT bertanggung jawab atas pengelolaan proses SMKI dan memberikan bimbingan pelaksanaan kepada seluruh karyawan dan pengajar. Penilaian risiko dilakukan secara berkala oleh PYDT untuk menentukan tindak lanjut yang diperlukan.

3. Kontrol Akses Keamanan Informasi

   PYDT memiliki kontrol akses keamanan informasi yang bertujuan untuk fokus pada aspek teknis, pemeliharaan aset, dan tingkat keamanan yang dimiliki, terutama dalam kondisi fisik. Standar ini berfungsi sebagai referensi lengkap dan sesuai untuk PYDT, yang belum pernah distandarisasi sebelumnya oleh ISO/IEC 27001. Diharapkan penerapan prosedur ini akan memberikan dampak positif, memungkinkan pengontrolan yang lebih baik terhadap keamanan informasi. Standar ini dianggap sebagai praktik terbaik dalam pemilihan kontrol keamanan informasi, yang sesuai dengan kebutuhan masing-masing di dalam organisasi untuk diterapkan dalam lingkungan bisnis organisasi tersebut.

4.3.3 Pengelolaan Risiko Keamanan Informasi

1. Penilaian Risiko

   Pada tahap ini penilaian risiko dilakukan untuk mengetahui seberapa besar dan identifikasi risiko apa yang akan diterima oleh PYDT jika informasi unit mendapat ancaman atau gangguan pada pengamanan informasi, yaitu:

   a. Dokumen ruang lingkup menjadi *input* dari proses penilaian risiko arena dokumen ruang lingkup menentukan sejauh mana identifikasi penilaian risiko yang akan dilakukan
   b. Penentuan kriteria penerimaan risiko dengan menggunakan metode matriks level risiko

2. Identifikasi Risiko

Identifikasi risiko ini bertujuan untuk mengetahui seberapa besar risiko yang akan diterima oleh organisasi. Proses identifikasi risiko ini memiliki 3 langkah, yaitu:

a. Langkah 1 : identifikasi aset dan klasifikasi aset yang ada pada PYDT dengan menggunakan tabel aset pada tabel 3.1.
b. Langkah 2 : menghitung nilai aset berdasarkan aspek keamanan informasi *(CIA)* dengan memberikan nilai masing-masing, setelah ini dihitung nilai asetnya yaitu dengan menggunakan persamaan matematis pada tabel 3.2.
c. Langkah 3 : menghitung nilai ancaman dan kelemahan aset.
    a. Membuat tabel kemungkinan kejadian atau gangguan keamanan *(Probability of Occurrence)* pada tabel 2.6
    b. Membuat tabel menghitung nilai ancaman dan menghitung nilai ancaman (NT)

3. Analisa dan Evaluasi Risiko

Analisa risiko ini bertujuan untuk mengetahui seberapa besar risiko yang akan diterima oleh organisasi. Proses identifikasi risiko ini memiliki 4 langkah, yaitu:

a. Langkah 1 : melakukan analisa dampak bisnis pada PYDT yang dilakukan dengan cara pembuatan tabel skala nilai *Business Impact Analysis* (BIA), setelah itu dibuat tabel BIA sesuai dengan fasilitas informasi yang dimiliki organisasi dengan mengacu pada tabel nilai skala BIA.
b. Langkah 2 : identifikasi level risiko dilakukan dengan membuat tabel matrik level risiko dengan menggunakan nilai probabilitas ancaman dan nilai BIA.
c. Langkah 3 : menentukan risiko diterima atau perlunya pengelolaan. Selanjutnya perlu ditentukan level risikonya dari hasil perhitungan matematis.

4.4 Implementasi Asesmen Risiko Keamanan Informasi

Tiga langkah dilakukan untuk menerapkan asesmen risiko ini: identifikasi risiko, analisis risiko, dan evaluasi risiko. Memberikan nilai tiap aset dari sisi dampak jika terjadi gangguan (*severity*) dan kemungkinan (*likelihood*) adalah bagian dari identifikasi risiko. Nilai kemungkinan dan dampak terjadi gangguan ditentukan berdasarkan wawancara dengan pemimpin Pondok Yatim Dhuafa Thursina.

4.4.1 Identifikasi Risiko dan Menghitung Nilai Aset

1. Identifikasi Aset

   Identifikasi aset di Pondok Yatim Dhuafa Thursina bertujuan untuk menentukan aset-aset yang digunakan untuk mendukung PYDT. Hasil observasi yang dilakukan dapat dikategorikan menjadi beberapa jenis aset, yaitu: *hardware*, *software* atau aplikasi, infrastruktur/jaringan, data atau informasi, dan sumber daya manusia (SDM).

Tabel 4 2 Aset Organisasi

Aset Organisasi		
No	Kategori Aset	Nama Aset
1.	*Hardware*	Komputer
		Laptop
		Sound System PC
		Printer
		Camera Digital
		Camera Logitech
		Proyektor
		Screen Proyektor
		Camera CCTV
2.	*Software*	Sistem Informasi

Aset Organisasi		
No	Kategori Aset	Nama Aset
1.	*Hardware*	Komputer
		Laptop
		Sound System PC
		Printer
		Camera Digital
		Camera Logitech
		Proyektor
		Screen Proyektor
		Camera CCTV
3.	Jaringan	WLAN
4.	Data	Data Anak Asuh
		Data Karyawan
		Data Pengajar
5.	Sumber Daya Manusia (SDM)	Karyawan
		Pengajar

Pada tabel diatas merupakan hasil identifikasi aset organisasi sebagai bagian dari implementasi asesmen risiko keamanan informasi pada PYD Thursina. Tabel ini mengkategorikan berbagai aset organisasi yang perlu dievaluasi dari perspektif risiko keamanan informasi. Berikut adalah penjelasan dari tabel tersebut:

1. Hardware (Perangkat Keras)
   - Komputer
   - Laptop
   - *Sound System* PC
   - *Printer*
   - *Camera Digital*

- *Camera Logitech*
- *Proyektor*
- *Screen Proyektor*
- *Camera* CCTV

2. *Software* (Perangkat Lunak)
   - Sistem Informasi
3. Jaringan (*Network*)
   - WLAN, jaringan nirkabel yang digunakan dalam organisasi.
4. Data
   - Data Anak Asuh
   - Data Karyawan
   - Data Pengajar
5. Sumber Daya Manusia (SDM)
   - Karyawan
   - Pengajar

Identifikasi aset seperti yang ditunjukkan pada tabel diatas merupakan langkah awal dalam proses asesmen risiko keamanan informasi. Dengan memahami aset yang dimiliki dan kategorinya, organisasi dapat mengidentifikasi potensi risiko dan mengembangkan strategi mitigasi yang sesuai untuk melindungi aset-aset tersebut dari berbagai ancaman. Berikut ini adalah tabel daftar ancaman dan kelemahan aset.

Tabel 4 3 Daftar Ancaman dan Kelemahan Aset

No	Kategori Aset	Daftar Aset	Ancaman dan Kelemahan
1.	*Hardware*	Laptop / Komputer	- Bencana alam - Kehilangan data - Kerusakan server - Pencurian komponen server - Kesalahan konfigurasi

2.	*Software*	Microsoft / Windows	- sistem tidak berjalan dengan normal - Serangan virus - Kesalahan konfigurasi dan *input* data pada sistem - Pembobolan sistem/akses ilegal - Sistem tidak dapat diakses
3.	Jaringan	Wifi , Kabel,	- Akses ilegal - Monopoly bandwidth - Serangan virus - Service down - Kerusakan hardware - Gangguan router - Hilangnya komponen hardware - Pembobolan jaringan
4.	Data	Karyawan, Anak Asuh	- Data hilang - Pencurian data - Data tidak dapat diakses - Data corrupt/rusak - Pencurian data - Akses ilegal
5.	Sumber Daya Manusia	Pengajar / Karyawan	- Penyalahgunaan data organisasi - Penyalahgunaan hak akses - Data tidak sesuai - Password shared

2. Nilai Aset

Setelah semua aset PYDT ditemukan, perhitungan dilakukan untuk mengetahui nilai masing-masing aset. Peneliti menghitung nilai aset berdasarkan tiga elemen keamanan informasi: kerahasiaan (rahasia), keutuhan (integritas), dan ketersediaan. Tabel berikut menunjukkan hasil penilaian aset PYDT untuk setiap komponen keamanan informasi.

Tabel 4 4 Nilai Aset Organisasi

No	Kategori Aset	Nama Aset	*Confidentiality* (NC)	Nilai *Integrity* (NI)	Nilai *Availability* (NA)	Nilai Aset
1.	*Hardware*	Komputer	1	1	3	5
		Laptop	1	1	3	5
		Sound System PC	1	0	2	3
		Printer	1	0	2	3
		Camera Digital	1	0	2	3
		Camera Logitech	1	0	2	3
		Proyektor	1	0	2	3
		Screen Proyektor	1	0	2	3
		Camera CCTV	1	2	3	6
2.	*Software*	Sistem Informasi	4	3	3	10
3.	Jaringan	WLAN	2	2	3	7
4.	Data	Data Anak Asuh	4	4	3	11
		Data Karyawan	3	3	2	8
		Data Pengajar	3	3	2	8
5.	Sumber Daya Manusia (SDM)	Karyawan	3	3	2	8
		Pengajar	4	3	3	10

Berikut penjelasan hasil dari nilai aset pada organisasi PYDT sebagai berikut:

1) Kategori *Hardware*

a. Komputer

Nilai Aset: *Confidentiality* (NC):1, *Integrity* (NI):, *Availability* (NA): 3, Total Nilai Aset: 5

b. Laptop

Nilai Aset: *Confidentiality* (NC): 1, *Integrity* (NI): 1, *Availability* (NA): 3, Total Nilai Aset: 5

c. Sound System PC

Nilai Aset: *Confidentiality* (NC): 1, *Integrity* (NI): 0, *Availability* (NA): 2, Total Nilai Aset: 3

d. Printer

Nilai Aset: *Confidentiality* (NC): 1, *Integrity* (NI): 0, *Availability* (NA): 2, Total Nilai Aset: 3

e. Camera Digital

Nilai Aset: *Confidentiality* (NC): 1, *Integrity* (NI): 0, *Availability* (NA): 2, Total Nilai Aset: 3

f. Camera Logitech

Nilai Aset: *Confidentiality* (NC): 1, *Integrity* (NI): 0. *Availability* (NA): 2, Total Nilai Aset: 3

g. Proyektor

Nilai Aset: *Confidentiality* (NC): 1, *Integrity* (NI): 2, *Availability* (NA): 2, Total Nilai Aset: 5

h. Screen Proyektor

Nilai Aset: *Confidentiality* (NC): 1, *Integrity* (NI): 0, *Availability* (NA): 2, Total Nilai Aset: 3

i. Camera CCTV

Nilai Aset: *Confidentiality* (NC): 1, *Integrity* (NI): 2, *Availability* (NA): 3, Total Nilai Aset: 6

2) Kategori *Software*

a. **S**istem Informasi

Nilai Aset: *Confidentiality* (NC): 4, *Integrity* (NI): 3, *Availability* (NA): 3, Total Nilai Aset: 10

3) Kategori Jaringan

a. WLAN

Nilai Aset: *Confidentiality* (NC): 3, *Integrity* (NI): 3, *Availability* (NA): 3, Total Nilai Aset: 9

4) Kategori Data

a. Data Anak Asuh

Nilai Aset: *Confidentiality* (NC): 4, *Integrity* (NI): 4, *Availability* (NA): 3, Total Nilai Aset: 11

b. Data Karyawan

Nilai Aset: *Confidentiality* (NC): 4, *Integrity* (NI): 3, *Availability* (NA): 2, Total Nilai Aset: 8

c. Data Pengajar

Nilai Aset: *Confidentiality* (NC): 3, *Integrity* (NI): 3, *Availability* (NA): 2, Total Nilai Aset: 8

5) Kategori SDM

a. Data Karyawan

Nilai Aset: *Confidentiality* (NC): 4, *Integrity* (NI): 3, *Availability* (NA): 2, Total Nilai Aset: 8

b. Data Pengajar

Nilai Aset: *Confidentiality* (NC): 4, *Integrity* (NI): 3, *Availability* (NA): 3, Total Nilai Aset: 10

Pada Sistem Informasi dan Pengajar memiliki nilai aset tertinggi (10), menunjukkan pentingnya perlindungan dan perhatian khusus pada area ini. Data Anak Asuh, Data Karyawan, dan Data Pengajar memiliki nilai aset yang tinggi (8), menunjukkan pentingnya menjaga kerahasiaan, integritas, dan ketersediaan data ini. Perangkat keras seperti Kamera *CCTV* dan Proyektor juga mendapat perhatian penting dengan nilai aset yang lebih tinggi dibanding perangkat keras lainnya. Perangkat keras lainnya (Komputer, Laptop, *Sound System PC*, Printer, *Camera*

Digital, dan lainnya) memiliki nilai aset yang lebih rendah, namun tetap memerlukan pengelolaan risiko yang memadai.

4.4.2 Analisis Risiko Keamanan Informasi

Prosedur Keamanan Informasi di Pondok Yatim Dhuafa Thursina (PYDT)

1. Identifikasi Kelemahan dan Ancaman
    a. Tujuan: Mengidentifikasi ancaman yang dapat membahayakan proses di PYDT
    b. Kelemahan: Merupakan ancaman terhadap ancaman informasi
    c. Tingkat Kerentanan: Ada berbagai tingkat kerentanan yang diidentifikasi.
2. Tahap Identifikasi Ancaman
    a. Definisi Ancaman: Kejadian yang dapat membahayakan sistem di PYDT
    b. Tujuan: Mengidentifikasi ancaman potensial dan dampaknya pada sistem
3. Penerapan Kode Praktik ISO/IEC 27001:2022
    a. Tujuan: Memaksimalkan pemeliharaan aset dan kontrol akses keamanan
    b. Proses : Kelemahan dan ancaman didaftarkan menggunakan kode praktik ini
4. Proses Identifikasi Risiko
    a. Data: Data dari proses identifikasi risiko digunakan untuk analisis risiko.
    b. Metode: Risiko dinilai berdasarkan nilai dampak dan gangguan untuk setiap aset.
5. Metode Analisis Risiko
    a. Proses: Analisis risiko menggunakan perkalian antara kemungkinan dan efek.
    b. Nilai Risiko: Berkisar antara 0 dan 25.
    c. Nilai Pengaruh: 0, 1, 2, 3, 4, 5.

6. Kategorisasi Nilai Risiko
    a. Nilai Rendah: 0 hingga 4
    b. Nilai Sedang: 5 hingga 9
    c. Nilai Tinggi: 10 hingga 16
7. Tabel Analisis Risiko
    a. Tabel 4.5 Menyampaikan hasil analisis risiko yang didasarkan pada perkalian nilai kemungkinan dan efek untuk setiap aset.

Dengan prosedur ini, PYDT dapat mengidentifikasi dan mengelola risiko yang ada pada sistem keamanan informasi mereka secara sistematis sesuai dengan standar ISO/IEC 27001:2022.

Tabel 4 5 Hasil Analisis Risiko

No	Aset Informasi	Ancaman	Kerentanan	Dampak	Kemungkinan	Tingkat Risiko	Mitagasi
1.	Data	Kebocoran Data	Keamanan sistem yang lemah	Tinggi	Sedang	Tinggi	Menggunakan enkripsi dan pengaturan akses
2.	Sistem Manajemen Informasi	Serangan *Malware*	Antivirus yang tidak diperbarui	Tinggi	Tinggi	Sangat Tinggi	Memperbarui antivirus dan *firewall*
3.	Hardware	Kerusakan Fisik	Penyimpanan tidak aman	Sedang	Rendah	Sedang	Menggunakan rak server dan pemeliharaan rutin
4.	Jaringan	Serangan *DDoS*	Proteksi jaringan yang tidak memadai	Tinggi	Sedang	Tinggi	Implementasi proteksi *DdoS*

Berdasarkan tabel hasil analisis risiko pada implementasi asesmen risiko keamanan informasi yang diberikan, berikut adalah penjelasan mengenai aset

informasi, ancaman, kerentanan, dampak, kemungkinan, tingkat risiko, dan langkah mitigasi yang diusulkan:

1. Data

- Ancaman: Kebocoran Data
- Kerentanan: Keamanan sistem yang lemah
- Dampak: Tinggi
- Kemungkinan**:** Sedang
- Tingkat Risiko**:** Tinggi
- Mitigasi: Menggunakan enkripsi dan pengaturan akses

Data menghadapi ancaman kebocoran karena sistem keamanan yang lemah. Dampak dari kebocoran data sangat tinggi, dan kemungkinan terjadinya juga sedang, sehingga tingkat risikonya tinggi. Langkah mitigasi yang diusulkan adalah dengan menggunakan enkripsi untuk melindungi data dan mengatur akses untuk mencegah akses yang tidak sah.

2. Sistem Manajemen Informasi

- Ancaman**:** Serangan Malware
- Kerentanan**:** Antivirus yang tidak diperbarui
- Dampak: Tinggi
- Kemungkinan: Tinggi
- Tingkat Risiko: Sangat Tinggi
- Mitigasi: Memperbarui antivirus dan *firewall*

Sistem manajemen informasi rentan terhadap serangan *malware* karena antivirus yang tidak diperbarui. Dampaknya sangat tinggi dan kemungkinan serangan juga tinggi, sehingga tingkat risikonya sangat tinggi. Langkah mitigasi yang disarankan adalah memperbarui antivirus dan *firewall* secara teratur untuk melindungi sistem dari serangan *malware*.

3. Hardware

- Ancaman: Kerusakan Fisik
- Kerentanan: Penyimpanan tidak aman
- Dampak: Sedang
- Kemungkinan**:** Rendah

- Tingkat Risiko: Sedang
- Mitigasi: Menggunakan rak server dan pemeliharaan rutin.

Hardware menghadapi ancaman kerusakan fisik karena penyimpanan yang tidak aman. Dampaknya sedang dan kemungkinan terjadinya rendah, sehingga tingkat risikonya sedang. Langkah mitigasi yang diusulkan adalah menggunakan rak server yang aman dan melakukan pemeliharaan rutin untuk mengurangi risiko kerusakan fisik.

4. Jaringan

- Ancaman: Serangan DdoS
- Kerentanan: Proteksi jaringan yang tidak memadai
- Dampak**:** Tinggi
- Kemungkinan: Sedang
- Tingkat Risiko: Tinggi
- Mitigasi: Implementasi proteksi DdoS

Jaringan rentan terhadap serangan DDoS karena proteksi jaringan yang tidak memadai. Dampaknya tinggi dan kemungkinan terjadinya sedang, sehingga tingkat risikonya tinggi. Langkah mitigasi yang disarankan adalah mengimplementasikan proteksi DDoS untuk melindungi jaringan dari serangan tersebut.

Langkah-langkah mitigasi yang diusulkan dalam *tabel* 4.5 bertujuan untuk mengurangi risiko yang terkait dengan aset informasi yang ada di organisasi. Setiap aset memiliki ancaman, kerentanan, dampak, dan kemungkinan yang berbeda, sehingga memerlukan tindakan mitigasi yang sesuai untuk memastikan keamanan informasi yang optimal.

Tabel 4 6 Hasil Asesmen Risiko tiap Aset

IDENTIFIKASI							PENILAIAN RISIKO			
No	***Asset Classfication***	**Lokasi**	**Nama Aset**	***Vulnerability***	***Threat***	***Impact***	***Likelihood* (Peluang Terjadi)**	***Saverity* (Dampak Kerugian)**	**Nilai Risiko dalam Angka**	**Nilai Risiko dalam Teks**
	Klasifikasi aset sesuai dengan lampiran 1. Organisasi, orang, fisik, dan teknologi			Kerentanan atau kelemahan aset dari sisi keamanan informasi	Ancaman dari dalam atau luar organisasi terhadap kerentanan	C: Confidentiality I: Integrity A: Availability	0 s.d 5	0 s.d 5	*Likelihood x Severity* (Peluang x Dampak Kerugian)	0 - 4 Rendah 5 - 9 Sedang 10 -16 Tinggi >16 Sangat Tinggi
1.	Teknologi	PYDT	*Hardware* (Laptop/Komputer)	Salah setting, Spesifikais rendah, kurang pemeliharaan	Hard disk penuh, sehingga komputer/laptop tidak dapat	I: Data Hilang/Rusak A: Sistem tidak dapat diakses	2	3	6	Sedang

IDENTIFIKASI							PENILAIAN RISIKO			
No	***Asset Classfication***	**Lokasi**	**Nama Aset**	***Vulnerability***	***Threat***	***Impact***	***Likelihood* (Peluang Terjadi)**	***Saverity* (Dampak Kerugian)**	**Nilai Risiko dalam Angka**	**Nilai Risiko dalam Teks**
					digunakan					
2.	Teknologi	PYDT	*Software* (Sistem Operasi MS Office atau aplikasi yang digunakan)	Windows mudah diganggu oleh virus/worm	Gangguan virus/worm dari internet	C: data rahasia terungkap I: data diubah A: sistem tidak dapat digunakan	5	4	20	Sangat Tinggi
3.	Teknologi	PYDT	Jaringan (Wifi /Perengkat	Salah setting, Spesifikais rendah,	Internet putus/ perangkat	A : Sistem tidak dapat digunaakn	3	1	3	Rendah

IDENTIFIKASI							PENILAIAN RISIKO			
No	***Asset Classfication***	**Lokasi**	**Nama Aset**	***Vulnerability***	***Threat***	***Impact***	***Likelihood* (Peluang Terjadi)**	***Saverity* (Dampak Kerugian)**	**Nilai Risiko dalam Angka**	**Nilai Risiko dalam Teks**
			gateway ke internet	kurang pemeliharaan	rusak	untuk akses jaringan				
4.	Fisik	PYDT	Data	Kontrol data yang tidak memadai, Enkripsi tidak ada atau lemah	Jaringan tidak aman, akses dapat dicuri	C: data rahasia terungkap I: data diubah A: sistem tidak dapat digunakan	2	3	6	Sedang
5.	Orang	PYDT	Karyawan atau Pengajar	Kurangnya prosedur, tidak ada pembatasan	Akses dapat dicuri, Ancaman dari dalam	I: Data Hilang/Rusak A: Sistem tidak dapat	2	3	6	Sedang

IDENTIFIKASI							PENILAIAN RISIKO			
No	***Asset Classfication***	**Lokasi**	**Nama Aset**	***Vulnerability***	***Threat***	***Impact***	***Likelihood* (Peluang Terjadi)**	***Saverity* (Dampak Kerugian)**	**Nilai Risiko dalam Angka**	**Nilai Risiko dalam Teks**
				akses yang memadai		diakses				

Penjelasan hasil asesmen risiko tiap Aset pada implementasi asesmen risiko keamanan informasi sebagai berikut ini :

1) *Hardware*
   - Klafikasi aset berupa teknologi (Laptop/Komputer)
   - Lokasi di PYDT
   - *Vulnerability*: Salah setting, spesifikasi rendah, kurang pemeliharaan
   - Threat: Ancaman dari dalam atau luar organisasi terhadap kerentanan
   - *Impact*: *Integrity* (I): Data hilang/rusak, *Availability* (A): Sistem tidak dapat diakses.
   - *Likelihood* (Peluang Terjadi): 2
   - *Severity* (Dampak Kerugian): 3
   - Nilai Risiko dalam Angka: 6
   - Nilai Risiko dalam Teks: Sedang
2) *Software* (Sistem Operasi MS Office atau aplikasi yang digunakan) (Teknologi)
   - Klafikasi aset berupa teknologi
   - Lokasi di PYDT
   - *Vulnerability:* Windows mudah diganggu oleh *virus/worm*
   - *Threat:* Gangguan *virus/worm* dari internet
   - *Impact*: *Confidentiality* (C): Data rahasia terungkap, *Integrity* (I): Data diubah**,** *Availability* (A): Sistem tidak dapat digunakan.
   - *Likelihood* (Peluang Terjadi): 5
   - *Severity* (Dampak Kerugian): 4
   - Nilai Risiko dalam Angka: 20
   - Nilai Risiko dalam Teks: Sangat Tinggi
3) Jaringan (*WiFi*/Perangkat *gateway* ke internet)
   - Klafikasi berupa teknologi
   - Lokasi di PYDT
   - *Vulnerability*: Salah setting, spesifikasi rendah, kurang pemeliharaan
   - *Threat*: Internet putus/perangkat rusak

- *Impact*: *Availability* (A): Sistem tidak dapat digunakan untuk akses jaringan.
- *Likelihood* (Peluang Terjadi): 1
- *Severity* (Dampak Kerugian): 3
- Nilai Risiko dalam Angka: 3
- Nilai Risiko dalam Teks**:** Rendah

Asesmen risiko ini menggambarkan tingkat kerentanan dan ancaman terhadap aset-aset di Pondok Yatim Dhuafa, serta dampaknya jika terjadi insiden keamanan. Risiko yang teridentifikasi diberi nilai berdasarkan peluang terjadinya dan dampaknya, menghasilkan klasifikasi risiko dalam angka dan teks untuk membantu dalam prioritas penanganan.

4.4.3 Evaluasi Risiko

Penilaian risiko dilakukan dalam dua tahap: pertama, memastikan apakah penilaian risiko sudah sesuai dengan teori dan rencana yang ada; kedua, memberikan rekomendasi kepada instansi atau organisasi mengenai aset yang perlu diprioritaskan untuk ditangani. Penilaian risiko dilakukan oleh penulis. Evaluasi risiko dimulai setelah nilai risiko untuk setiap aset ditentukan dalam proses analisis risiko. Evaluasi ini telah selesai dan telah sesuai dengan teori serta rencana. Penulis merekomendasikan kepada PYDT agar aset teknologi, seperti sistem operasi, diprioritaskan untuk ditangani karena memiliki nilai risiko tinggi, sehingga perlu dilakukan tindakan untuk menurunkan nilai risiko tersebut. Metode yang digunakan dalam proses evaluasi risiko ini adalah kualitatif, dengan menghubungkan hasil penilaian dengan teori yang digunakan dalam penelitian ini. Hasil evaluasi risiko dijelaskan dalam *tabel* 4.7 yang mencantumkan daftar prioritas penanganan risiko.

Tabel 4 7 Daftar Prioritas Penangan

No	Nama Aset	Kategori Aset	Prioritas Risiko
1	*Software* (Sistem Operasi MS *Office* atau aplikasi dan layanan yang digunakan)	Teknologi	1

Pada gambar tersebut, terlihat tabel hasil dari Daftar Prioritas Penanganan evaluasi risiko pada Implementasi Asesmen Risiko Keamanan yaitu:

a. Prioritas risiko "1" menunjukkan bahwa aset tersebut memiliki tingkat risiko yang sangat tinggi dan memerlukan penanganan segera.
b. Risiko tinggi pada software mungkin disebabkan oleh beberapa faktor seperti kerentanan keamanan, pentingnya software tersebut bagi operasi bisnis, atau dampak yang signifikan jika terjadi insiden keamanan.

Dari tabel berikut dapat dilihat bahwa *software* yang termasuk dalam kategori teknologi memiliki prioritas risiko tertinggi dan memerlukan penanganan segera untuk mengurangi atau mengelola risiko tersebut. Dalam evaluasi risiko yang dilakukan di Pondok Yatim Dhuafa Thursina Bogor, aset teknologi seperti sistem operasi telah diidentifikasi sebagai komponen dengan nilai risiko tinggi. Evaluasi ini mencakup proses identifikasi, analisis, dan penilaian risiko yang menyeluruh terhadap semua aset teknologi yang dimiliki oleh lembaga.

Hasil evaluasi tersebut kemudian disusun dalam tabel daftar prioritas penanganan yang bertujuan untuk membantu dalam menentukan langkah-langkah mitigasi yang perlu diambil berdasarkan tingkat risiko masing-masing aset.

1. Identifikasi Risiko
    a. Proses identifikasi risiko melibatkan penentuan aset teknologi yang ada, seperti sistem operasi, perangkat keras, perangkat lunak, dan jaringan.
    b. Risiko terkait masing-masing aset diidentifikasi, termasuk ancaman dan kerentanannya.
3. Analisis Penilaian Risiko
    a. Analisis risiko dilakukan untuk menilai dampak dan kemungkinan terjadinya setiap risiko yang telah diidentifikasi.

b. Sistem operasi dinilai memiliki nilai risiko tinggi karena merupakan komponen kritis yang mendukung operasional lembaga.

4. Evaluasi Risiko
    a. Hasil analisis risiko menunjukkan bahwa sistem operasi memiliki dampak yang signifikan terhadap keberlangsungan operasional lembaga jika terjadi insiden keamanan.
    b. Evaluasi ini mengindikasikan perlunya prioritas tinggi dalam penanganan risiko terhadap sistem operasi.
5. Tabel Daftar Prioritas Penanganan
    a. Dalam tabel daftar prioritas penanganan, aset teknologi yang memiliki nilai risiko tinggi yaitu sistem operasi ditempatkan pada posisi prioritas utama.
    b. Penanganan risiko terhadap sistem operasi mencakup langkah-langkah mitigasi seperti pembaruan rutin, patching keamanan, dan monitoring berkelanjutan untuk memastikan sistem operasi tetap aman.
6. Tindakan Mitigasi
    a. Tindakan mitigasi yang diambil bertujuan untuk mengurangi dampak dan kemungkinan terjadinya risiko.
    b. Implementasi kontrol keamanan tambahan, seperti *firewall* dan sistem deteksi intrusi, juga dapat dilakukan untuk melindungi sistem operasi.

Dengan menetapkan sistem operasi sebagai prioritas utama dalam penanganan risiko, Pondok Yatim Dhuafa Thursina Bogor dapat mengurangi potensi kerugian dan memastikan kelangsungan operasional lembaga. Penerapan langkah-langkah mitigasi yang tepat akan membantu menurunkan nilai risiko dan meningkatkan keamanan informasi yang dikelola.

4.5 Evaluasi Hasil Asesmen Risiko Keamanan Informasi

Dalam pengelolaan risiko SMKI (Sistem Manajemen Keamanan Informasi), hasil yang diharapkan adalah terbentuknya aset dan nilai yang dapat

diandalkan, serta hasil analisis dan evaluasi risiko yang diperlukan oleh Pondok Yatim Dhuafa Thursina (PYDT) dalam tahap awal penerapan SMKI. Setelah implementasi selesai, dilakukan pengujian menggunakan metode UAT (*User Acceptance Test*) untuk mengevaluasi hasil pengelolaan risiko terkait keamanan informasi. Pengujian ini mencakup identifikasi risiko, analisis penilaian risiko, dan evaluasi risiko. Mengevaluasi dan memprioritaskan risiko berdasarkan analisis penilaian yang telah dilakukan. Langkah ini membantu menentukan tindakan pengelolaan risiko yang paling efektif.

Setelah proses UAT, PYDT menyatakan bahwa hasil pengelolaan risiko sesuai dengan poin-poin yang ditentukan atau ditetapkan selama proses wawancara. Hal ini menunjukkan bahwa pengelolaan risiko yang dilakukan dapat memenuhi kebutuhan lembaga dalam menerapkan SMKI. Meskipun hasil pengelolaan risiko ini sudah memadai untuk tahap awal penerapan SMKI, penelitian ini mengindikasikan perlunya pengembangan lebih lanjut. Untuk melakukan asesmen risiko keamanan informasi secara menyeluruh, perlu ada penelitian lanjutan yang mencakup:

1) Penanganan Risiko

   Melibatkan identifikasi langkah-langkah mitigasi atau pengendalian yang harus diambil untuk mengurangi dampak dan kemungkinan terjadinya risiko. Penanganan risiko adalah langkah penting dalam memastikan bahwa semua risiko yang diidentifikasi dan dinilai dapat dikelola dengan efektif

2) Keamanan Informasi pada Sistem Informasi

   Melakukan evaluasi menyeluruh terhadap sistem informasi yang digunakan di PYDT, memastikan bahwa semua aspek keamanan informasi telah diatasi dengan baik.

Penelitian lanjutan ini akan membantu PYDT dalam mencapai kepatuhan penuh terhadap standar ISO/IEC 27001:2022 dan memastikan bahwa SMKI yang diterapkan benar-benar efektif dalam melindungi informasi penting dan sensitif.

Evaluasi hasil asesmen risiko diberikan untuk PYDT adalah segera memulai implementasi perencanaan SMKI berdasarkan standar ISO 27001. Langkah-langkah yang perlu dilakukan antara lain adalah menentukan ruang lingkup SMKI,

menetapkan kebijakan SMKI, dan mengelola risiko keamanan informasi. Selain itu, PYDT juga perlu melakukan penanganan risiko secara menyeluruh dan melakukan evaluasi terhadap sistem informasi yang digunakan. Hal ini bertujuan untuk memastikan bahwa semua aspek keamanan informasi telah diatasi dengan baik.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan terkait dengan perencanaan Sistem Manajemen Keamanan Informasi berdasarkan Standar ISO/IEC 27001:2022 pada Pondok Yatim Dhuafa Thursina Bogor, dapat disimpulkan sebagai berikut :

1. Pondok Yatim Dhuafa Thursina Bogor telah menerapkan standar ISO/IEC 27001:2022 dalam mengelola risiko keamanan. Proses ini melibatkan pengidentifikasian, analisis, dan evaluasi risiko secara terstruktur dan komprehensif. Hasilnya menunjukkan kemampuan lembaga ini dalam mengenali dan mengevaluasi risiko keamanan informasi dengan efisien, serta merancang langkah-langkah mitigasi yang sesuai untuk mengurangi dampak dan kemungkinan terjadinya risiko. Penerapan standar ini memberikan kerangka kerja yang terstruktur dan sistematis, yang membantu dalam menjaga keamanan informasi yang dikelola.
2. Penilaian manajemen risiko keamanan di Pondok Yatim Dhuafa Thursina Bogor, yang melibatkan identifikasi risiko, analisis risiko, dan evaluasi hasil risiko, telah dilakukan sesuai dengan pedoman ISO/IEC 27001:2022. Hasil penilaian menunjukkan bahwa langkah-langkah manajemen risiko yang diterapkan telah memenuhi kebutuhan dan persyaratan lembaga dalam menjaga keamanan informasi. Evaluasi ini menyoroti pentingnya pengujian dan pemantauan yang berkelanjutan untuk memastikan efektivitas tindakan mitigasi yang telah dijalankan. Dengan mengikuti standar ISO/IEC 27001:2022, Pondok Yatim Dhuafa Thursina Bogor dapat meningkatkan perlindungan terhadap informasi sensitif yang dikelola, serta memperkuat kepercayaan dan reputasi lembaga di mata donatur dan masyarakat.

5.2 Saran

Berdasarkan penelitian yang telah dilakukan peneliti yaitu dalam mengelola risiko Sistem Manajemen Keamanan Informasi (SMKI) dan menerapkan ISO/IEC 27001:2022 pada Pondok Yatim Dhuafa Thursina. Oleh karena itu, peneliti mencoba memberikan saran untuk penelitian selanjutnya sebagai berikut:

1. Untuk mencapai kepatuhan penuh dan efektivitas SMKI, diperlukan penelitian lanjutan yang fokus pada penanganan risiko dengan mengidentifikasi langkah-langkah mitigasi atau kontrol.
2. Disarankan bagi peneliti selanjutnya untuk melakukan evaluasi menyeluruh terhadap sistem informasi di PYDT dapat memastikan semua aspek keamanan informasi tertangani dengan baik.
3. Dalam penelitian selanjutnya dapat melakukan dengan langkah-langkah yang perlu diambil meliputi menetapkan cakupan SMKI, merumuskan kebijakan SMKI, dan mengelola risiko keamanan informasi secara komprehensif. Dengan langkah-langkah tersebut, PYDT dapat memberikan perlindungan optimal terhadap data sensitif yang dikelola.

DAFTAR PUSTAKA

[1] A. Chopra and M. Chaudhary, “The need for information security,” in *Implementing an Information Security Management System*, Berkeley, CA: Apress, 2019, pp. 1–20. Accessed: Jun. 13, 2024. [Online]. Available: http://dx.doi.org/10.1007/978-1-4842-5413-4_1

[2] “Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines”, doi: 10.3403/30351736.

[3] A. Tsohou, M. Karyda, and S. Kokolakis, “Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs,” *Computers & Security*, vol. 52, pp. 128–141, Jul. 2015, doi: 10.1016/j.cose.2015.04.006.

[4] S. A and B. J, “Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines,” *Journal of Information Privacy and Security*, 2021, doi: 10.3403/30351736.

[5] M. I. Muhyi Maulani, S.Kom, “Pondok Yatim Dhuafa Thursina,” *Pondok Yatim Dhuafa Thursina*, Jul. 15, 2020. https://www.pydthursina.org (accessed Jun. 13, 2024).

[6] “Jurnal ICT: Information Communication & Technology.” https://ejournal.ikmi.ac.id/index.php/jict-ikmi

[7] A. Y. Rukmana *et al.*, *PENGANTAR SISTEM INFORMASI : Panduan Praktis Pengenalan Sistem Informasi & Penerapannya*. PT. Sonpedia Publishing Indonesia, 2023.

[8] Y. B. Nizar, “TA : Perencanaan Sistem Manajemen Keamanan Informasi Berdasarkan Standar ISO/IEC 27001:2013 pada PT Angkasa Pura 1 (Persero) Surabaya,” *Repositori Universitas Dinamika*, Jan. 01, 2021. https://repository.dinamika.ac.id/id/eprint/5923/

[9] W. A. Pratiwi, “TA : Perencanaan Sistem Manajemen Keamanan Informasi Berdasarkan Standar ISO 27001:2013 pada Kominfo Provinsi Jawa

Timur,"*Repositori Universitas Dinamika*, Jan.01,2019. https://repository.dinamika.ac.id/id/eprint/3310/ (accessed Jun. 13, 2024).

[10] N. F. Octariza, "Analisis sistem manajemen keamanan informasi menggunakan standar iso/Iec 27001 dan iso/lec 27002 pada kantor pusat pt jasamar,"Feb.21,2019.https://repository.uinjkt.ac.id/dspace/handle/123456789/48163 (accessed Jun. 13, 2024).

[11] A. Y. Rukmana *et al.*, *PENGANTAR SISTEM INFORMASI : Panduan Praktis Pengenalan Sistem Informasi & Penerapannya*. PT. Sonpedia Publishing Indonesia, 2023.

[12] M. K. Sari, Y. Saintika, and W. A. Prabowo, "Penyusunan Manajemen Risiko Keamanan Informasi Dengan Standar ISO 27001 Studi Kasus Institut Teknologi Telkom Purwokerto," *Jurnal Sistem dan Teknologi Informasi (JustIN)*, vol. 10, no. 4, p. 423, Dec. 2022, doi: 10.26418/justin.v10i4.48977.

[13] F. Nisa, M. Megawati, M. L. Hamzah, and I. Maita, "Analisis Manajemen Risiko Keamanan Sistem BMKGSoft Menggunakan Metode OCTAVE-S," *Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi*, vol. 8, no. 1, p. 62, Feb. 2022, doi: 10.24014/rmsi.v8i1.14334.

[14] Drs. Rusmanto, "SNI ISO IEC 27001-2022," *Hak cipta Badan Standardisasi Nasional, SNI ISO IEC 27001-2022. Salinan standar ini dibuat oleh BSN, untuk Drs. Rusmanto | STTNF |*. 2023.

[15] Drs. Rusmanto, *Modul Kuliah Sistem Manajemen Keamanan Informasi Berdasarkan SNI ISO/IEC 27001*. 2023.

[16] Sarno, R. 2009. *Sistem Manajemen Keamanan Informasi berbasis ISO 27001*. *Surabaya*: ITSPress.

[17] Ardyan, E., Boari, Y., Akhmad, A., Yuliyani, L., Hildawati, H., Suarni, A., ... & Judijanto, L. (2023). *Metode Penelitian Kualitatif dan Kuantitatif: Pendekatan Metode Kualitatif dan Kuantitatif di Berbagai Bidang*. PT. Sonpedia Publishing Indonesia.

LAMPIRAN

Hari/Tanggal : 7 Juni 2024

Tempat : Zoom Meeting (Online)

Narasumber : Bapak Ikbar Muhyi Maulani, S.Kom, M.Pd.

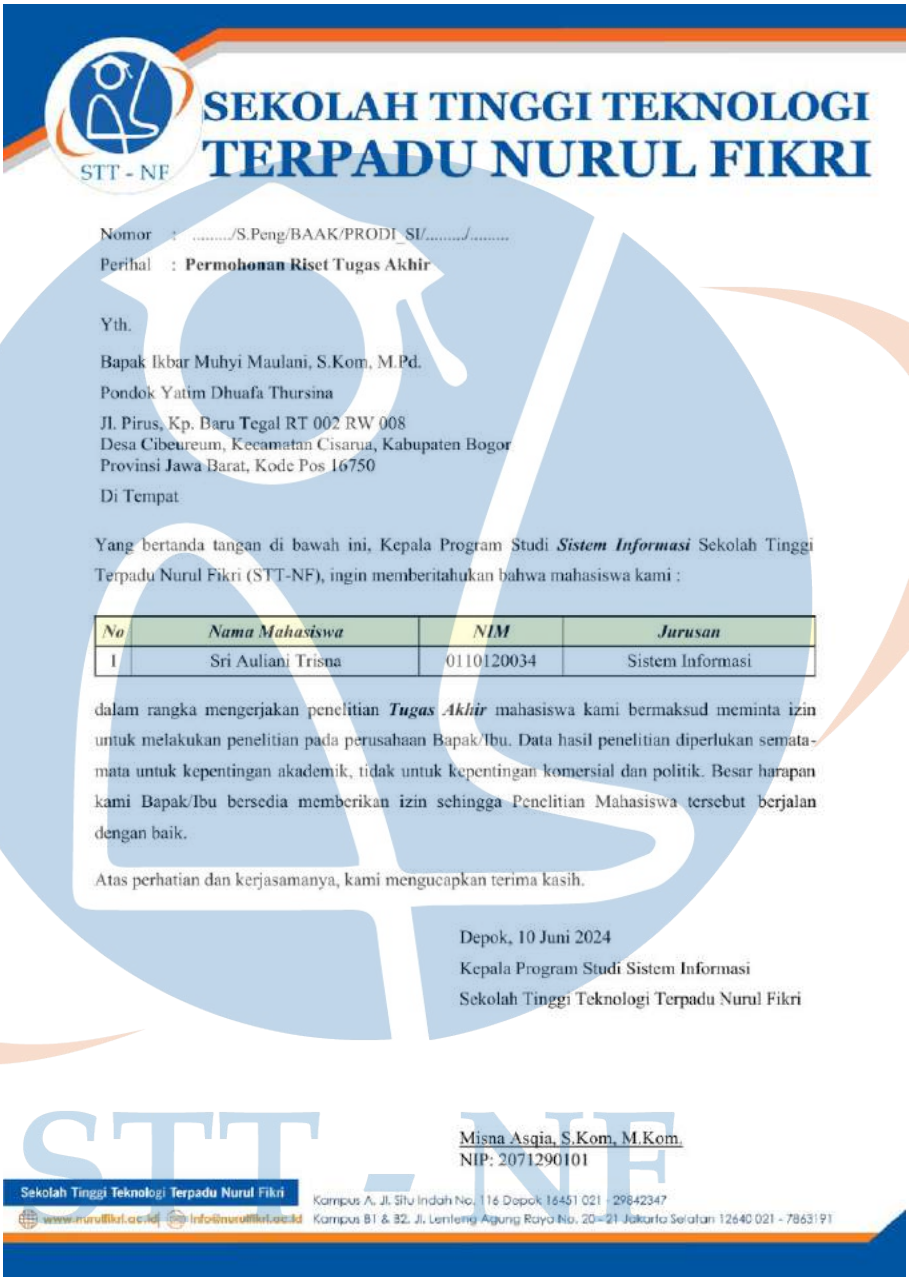
Jabatan : Pimpinan Pondok Yatim Dhuafa Thursina

Hasil Wawancara		
P	:	Kepada Pak Ikbar selaku Pimpinan PYDT, ingin bertanya pak. Apakah pondok yatim dhuafa ini sudah menerapkan sistem manajemen keamanan informasi? Jika ya, sejak kapan?
N	:	Untuk sistem manajemen keamanan informasi, kami belum ada sistem keamanan perihal yang dimaksud dalam penelitian ini.Jika dalam penelitian ini dapat membantu dalam membentuk sistem keamanan informasi, Insha Allah kita bisa aware ataupun bisa menerima masukan masukan dan apa yang harus dilakukan dalam suatu lembaga ketika ada teknologi yang harus dijaga pada keamanan informasi.
P	:	Selanjutnya, Apakah selama belum ada keamanan sistem informasi ada insiden atau pernah terjadi pada sistem informasi di pondok yatim dhuafa? Jika ya, bagaimana penanganannya?
N	:	Selama ini, Alhamdulilah belum ada kendala atau pernah terjadi seperti kehilangan data, ke hack atau kesalahan data.
P	:	Jika berkenan dan boleh usul, untuk dalam sistem informasi pada PYDT ini dapat menerapkan manajemen keamanan informasi yang sesuai dengan ISO/IEC 27001 ?
N	:	Sebelumnya dari saya sangat berterima kasih ya, kalau dalam penelitian ini mau bantu dalam menerapkan sistem keamanan informasi pada lembaga ini, karena kita belum ke arah sana. Dan harapannya bisa menerapkan dalam menjaga sistem

		keamanan informasi yang ada di pondok ini.
P	:	Dalam penyusunan awal dalam SMKI, sekiranya Apa yang dibutuhkan dari PYDT khususnya pada sistem informasi ini?
N	:	Pada penyusunan awal terkait penerapan ISO 27001 terkait penyusunan dokumen yang belum terstruktur dan terarah.
P	:	Dari perencanaan penyusunan pada penilain risiko dibutuhkannya beberapa poin, yang pertama itu adalah ruang lingkup yang sesuai dengan konteks organisasi. Kemudian yang kedua itu ada menentukan kebijakan dari organisasi itu sendiri dan yang terakhir penilain risiko pada PYDT
N	:	Pada proses pengembangan sistem yang menjadi ruang lingkup pada penerapan SMKI yang berkaitan dengan sistem informasi PYDT, dengan ini harapannya dapat lebih spesifik pada pengembangan sistem informasi dan implementasi dengan ISO 27001 ini dimulai pada SMKI
P	:	Pada ketentuan kebijakan dari PYDT itu sendiri dalam menerapkan manajemen keamanan informasi yang berkaitan dengan sistem informasi Pengelolaan Risiko, untuk kebijakannya seperti apa ya pak ?
N	:	Untuk meningkatkan kepercayaan masyarakat terhadap PYDT mengenai keamanan data dan informasi, institusi perlu mendapatkan sertifikasi standar ISO 27001. Dalam upaya menerapkan kebijakan ini, perlu adanya penyusunan kebijakan yang melibatkan penerapan standar tersebut. Namun, sebelum menerapkan standar ini kepada seluruh karyawan atau pengajar, PYDT saat ini fokus pada pengembangan sistem, khususnya sistem informasi keamanan.

LAPORAN DOKUMEN

1. Surat izin penelitian



SEKOLAH TINGGI TEKNOLOGI
TERPADU NURUL FIKRI
STT - NF

Nomor : ...../S.Peng/BAAK/PRODI_SI/...../.....
Perihal : **Permohonan Riset Tugas Akhir**

Yth.

Bapak Ikbar Muhyi Maulani, S.Kom, M.Pd.
Pondok Yatim Dhuafa Thursina
Jl. Pirus, Kp. Baru Tegal RT 002 RW 008
Desa Cibeureum, Kecamatan Cisarua, Kabupaten Bogor
Provinsi Jawa Barat, Kode Pos 16750
Di Tempat

Yang bertanda tangan di bawah ini, Kepala Program Studi ***Sistem Informasi*** Sekolah Tinggi Terpadu Nurul Fikri (STT-NF), ingin memberitahukan bahwa mahasiswa kami :

No	*Nama Mahasiswa*	*NIM*	*Jurusan*
1	Sri Auliani Trisna	0110120034	Sistem Informasi

dalam rangka mengerjakan penelitian ***Tugas Akhir*** mahasiswa kami bermaksud meminta izin untuk melakukan penelitian pada perusahaan Bapak/Ibu. Data hasil penelitian diperlukan semata-mata untuk kepentingan akademik, tidak untuk kepentingan komersial dan politik. Besar harapan kami Bapak/Ibu bersedia memberikan izin sehingga Penelitian Mahasiswa tersebut berjalan dengan baik.

Atas perhatian dan kerjasamanya, kami mengucapkan terima kasih.

Depok, 10 Juni 2024
Kepala Program Studi Sistem Informasi
Sekolah Tinggi Teknologi Terpadu Nurul Fikri

Misna Asqia, S.Kom, M.Kom.
NIP: 2071290101

Sekolah Tinggi Teknologi Terpadu Nurul Fikri
www.nurulfikri.ac.id info@nurulfikri.ac.id
Kampus A. Jl. Situ Indah No. 116 Depok 16451 021 - 29842347
Kampus B1 & B2. Jl. Lenteng Agung Raya No. 20-21 Jakarta Selatan 12640 021 - 7863191

2. Profil LKSA – Pondok Yatim Dhuafa

3. Proses Wawancara bersama Bapak M. Ikbar Muhyi Maulani S.Kom, M.Pd. Selaku Pimpinan Pondok Yatim Dhuafa Thursina.

https://drive.google.com/file/d/1q06MPfSJphFtx5zaYHwkXyivJXtLzGuH/view?usp=drive_link