PROPOSAL SKRIPSI

SISTEM PAKAR UNTUK RISK ASSESSMENT KEAMANAN SISTEM INFORMASI BERDASARKAN ISO 27002 DENGAN METODE CERTAINTY FACTOR

Disusun oleh:

Nama : Denny Hadi Pratama
NIM : 1912038

PROGRAM STUDI TEKNOLOGI INFORMASI-S1

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MULIA

BALIKPAPAN

2023

HALAMAN PERSETUJUAN

SISTEM PAKAR UNTUK RISK ASSESSMENT KEAMANAN SISTEM INFORMASI BERDASARKAN ISO 27002 DENGAN METODE CERTAINTY FACTOR

Dipersiapkan dan Disusun oleh

Denny Hadi Pratama

1912038

Telah disetujui oleh Tim Dosen Pembimbing Skripsi
pada tanggal, 24 Juni 2023

Pembimbing Utama	Pembimbing Pendamping
Gunawan, S.T., M.T	**Wahyu Nur Alimyaningtiyas, S.Kom., M.Kom**
NIDN 1122047201	**NIDN 1103028801**

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1.Latar Belakang

Dalam era digital yang terus berkembang, keamanan sistem informasi menjadi salah satu perhatian utama bagi perusahaan dan organisasi di seluruh dunia. Dengan adanya serangan siber yang semakin kompleks dan canggih, kerentanan terhadap pelanggaran keamanan dan pencurian data menjadi ancaman yang serius. Oleh karena itu, perusahaan dan organisasi perlu menerapkan langkah-langkah yang tepat untuk mengevaluasi dan mengelola risiko keamanan pada sistem informasi.

Menurut (Disterer, G., 2013) ISO 27002 atau *Information Security Management System* merupakan standar internasional yang mengatur praktik-praktik keamanan informasi yang harus diterapkan dalam sebuah organisasi. Namun, ISO 27002 membutuhkan keahlian khusus dalam menganalisis dan menginterpretasi data risiko yang kompleks.

Dalam hal ini, Sistem Pakar hadir sebagai solusi yang menjanjikan untuk membantu organisasi dalam menghadapi tantangan risk assessment keamanan sistem informasi. Dengan pendekatan metode *certainty factor* penilaian risiko dapat diberikan dengan tingkat kepastian yang lebih tinggi, karena mempertimbangkan berbagai faktor dan kondisi yang mempengaruhi tingkat risiko.

1.2.Rumusan Masalah

Berdasarkan latar belakang masalah diatas, maka permasalahan yang akan dibahas/diteliti adalah sebagai berikut:

a. Bagaimana cara menerapkan ISO 27002 dalam membangun sistem pakar untuk Keamanan Sistem Informasi?
b. Bagaimana membangun sebuah sistem pakar yang dapat dijadikan sebagai alat untuk membantu dalam proses penentuan risiko sistem informasi dengan metode Certainty Factor ?

1.3.Batasan Masalah

Adapun batasan masalah dalam penelitian ini sebagai berikut:

a. Hasil akhir penelitian ini berupa sistem pakar yang digunakan untuk proses penilaian pada setiap *assesment* dengan standar ISO 27002.
b. Metode yang digunakan dalam sistem pakar menggunakan metode Certainty Factor.
c. Bahasa Pemrograman yang digunakan dalam membangun sistem ini menggunakan PHP dan Basis Data MySQL.
d. Pengujian yang dilakukan hanya pada sebatas pengujian sistem yang dibangun dengan fitur fitur yang sudah ada dengan metode Blackbox testing dan WhiteBox Testing.

1.4.Tujuan Penelitian

Adapun tujuan penelitian dalam penelitian ini sebagai berikut:

a. Membangun sebuah sistem pakar yang dapat digunakan sebagai alat untuk proses penilaian risiko dalam pemenuhan aspek sistem manajemen keamanan sistem informasi.
b. Memberikan informasi kepada pengguna mengenai aspek yang dibutuhkan untuk keamanan sistem informasi.
c. Sebagai salah satu syarat kelulusan pada Program Studi Teknologi Informasi Universitas Mulia Balikpapan.

1.5.Manfaat Penelitian

Adapun manfaat penelitian dalam penelitian ini sebagai berikut:

a. Menghasilkan sebuah sistem pakar yang dapat dimanfaatkan sebagai alat untuk proses penilaian risiko organisasi dalam pemenuhan aspek sistem manajemen keamanan sistem informasi.
b. Mampu memberikan alternatif bagi pengguna dalam menerapkan penggunaan ISO 27002 dalam sebuah organisasi.
c. Memberikan kontribusi pada perkembangan keamanan sistem informasi dengan menyediakan data yang valid dan akurat terkait metode Certainty Factor dalam proses *risk assessment*.

BAB II

LANDASAN TEORI

2.1.Tinjauan Pustaka

Dalam tinjauan pustaka akan dibahas mengenai penelitian - penelitian terdahulu yang pernah dilakukan peneliti sebelumnya. Dalam tinjauan pustaka ini penelitian yang terkait berupa sistem pakar dan penelitian terkait ISO 27002. Dalam penelitian yang dilakukan oleh (Andriyanto, 2014) dalam jurnal penelitiannya dengan judul "Sistem Pakar Untuk Risk Assessment Keamanan Sistem Informasi Berdasarkan Iso 27002 Dengan Metode Forward Chaining", mempunyai tujuan untuk membangun sebuah sistem pakar untuk mengetahui posisi atau tingkat keamanan dari sebuah perusahaan dengan melakukan risk assessment. Hasil dari penelitian ini mengemukakan sistem pakar yang diusulkan memiliki tingkat kesesuaian hasil risk assessment mencapai 87,72%. Kesimpulan yang didapat adalah dengan adanya integrasi antara risk assessment dengan sistem pakar, maka dapat diketahui gambaran posisi tingkat keamanan suatu organisasi dan juga dapat membantu untuk menentukan perlu tidaknya organisasi untuk melakukan audit terhadap keamanan sistem informasi.

Penelitian kedua yang dilakukan oleh (Tanuwijaya, 2022) dengan judul penelitian "Analisis Keamanan Sistem Informasi Perdagangan Terintegrasi Menggunakan Standar ISO 27002" menunjukkan pendekatan PT. XYZ terhadap keamanan Sipeter tidak konsisten dan kontrol keamanan dilakukan secara informal. Hal ini ditunjukan dengan maturity level Sipeter adalah 1.55 atau level Initial.

Tujuan dari penelitian ini untuk menganalisis object keamanan Sipeter Menggunakan standar ISO 27002 pada klausul 8 sampai dengan klausul 14.

Penelitian ketiga yang dilakukan oleh (Syahputra, 2022) dalam jurnal penelitiannya yang berjudul "Perancangan Sistem Pakar untuk Mengidentifikasi Keamanan Transaksi Online Website E-commerce dengan Menggunakan Metode Certainty Factor", menjelaskan tujuan dari penelitian ini untuk membuat sistem pakar deteksi keamanan sistem informasi dengan gejala atau aturan yang ada. Hasil penelitian ini berupa sistem pakar yang menghasilkan keluaran berupa kemungkinan website terancam keamanannya atau tidak. Sistem ini juga menampilkan besarnya tingkat risiko keamanan website. Besarnya nilai risiko tersebut merupakan hasil perhitungan dengan menggunakan metode Certainty Factor.

Penelitian keempat yang dilakukan oleh (Denda, dkk, 2022) dengan judul "Implementasi Algoritma Certainty Factor pada Sistem Pakar untuk Mendeteksi Kecanduan Online Games" mempunyai tujuan membuat sebuah sistem berbasis Android untuk mendeteksi kecanduan bermain games online dengan metode certainty factor (CF). Hasil pengujian akurasi berdasarkan 18 sampel data acak menunjukkan nilai 83%. Penelitian berikutnya dibutuhkan pengetahuan yang didapat dari beberapa pakar dan menyarankan untuk menggunakan algoritma lain sebagai pembanding dalam satu sistem.

Penelitian kelima yang dilakukan oleh (Aldisa, 2022) dengan judul "Penggunaan Metode Certainty Factor pada Sistem Pakar Deteksi Kerusakan Perangkat Keras (Hardware) Komputer di Laboratorium Berbasis Android"

bertujuan untuk menghasilkan sebuah sistem pakar berbasis android untuk diagnosa akhir keadaan dengan menggunakan metode certainty factor. Sistem ini dapat memberikan informasi mengenai 4 macam jenis diagnosa kerusakan, 12 data gejala kerusakan. Hasil pengujian menggunakan Alpha Test terhadap 20 peserta diperoleh pilihan jawaban “cocok” dengan nilai persentase 54%.

2.2.Keaslian Penelitian

Tabel 2.1 Matriks Literatur Review dan Posisi Penelitian Judul Skripsi

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
1.	*Sistem Pakar Untuk Risk Assessment Keamanan Sistem Informasi Berdasarkan Iso 27002 Dengan Metode Forward Chaining*	Andriyanto, F., digilib.uns.ac.id, 2014	Membangun sebuah sistem pakar untuk mengetahui posisi atau tingkat keamanan dari sebuah risiko dengan melakukan risk assessment	Dengan adanya integrasi antara risk assessment dengan sistem pakar, maka dapat diketahui gambaran posisi tingkat keamanan suatu perusahaan dan juga dapat membantu untuk menentukan perlu tidaknya perusahaan untuk melakukan audit terhadap keamanan sistem informasi.	Penelitian yang direview memiliki kelemahan pada metode Forward chaining dengan aturan yang mengharuskan pengguna mengikuti alur yang sudah dibuat, jika tidak ada maka tidak akan ditemukan hasilnya.	Perbandingan penelitian yang akan dilakukan dengan metode yang berbeda yaitu akan menggunakan metode CF dengan nilai CF yang sudah dikonsultasikan dengan aturan pakar.
2.	*Analisis Keamanan Sistem Informasi Perdagangan Terintegrasi Menggunakan Standar ISO 27002*	Tanuwijaya, H., Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi, 2022	Menganalisis object untuk dilakukan analisis keamanan Sipeter menggunakan standar ISO 27002 pada	Hasil penelitian menunjukkan pendekatan PT. XYZ terhadap keamanan Sipeter tidak konsisten dan kontrol keamanan yang dilakukan secara informal. Hasil ini ditunjukan dengan	Penelitian yang direview menggunakan object penelitian yang samar dan hanya sampai pada tahap analisis data.	Penelitian yang akan dilakukan yakni membangun sebuah sistem pakar dengan metode certainty factor dengan memanfaatkan domain yang ada.

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
			klausul 8 sampai dengan klausul 14.	maturity level Sipeter adalah 1.55 atau level Initial.		
3.	*Perancangan Sistem Pakar Untuk Mengidentifikasi Keamanan Transaksi Online Website E-commerce Dengan Menggunakan Metode Certainty Factor*	Syahputra, H., Informasi dan Teknologi Ilmiah (INTI), 2021	Membuat sistem pakar untuk deteksi keamanan sistem informasi dengan gejala atau aturan yang ada.	Hasil penelitian ini berupa Sistem Pakar yang menghasilkan keluaran berupa kemungkinan website dalam ancaman atau tidak. Sistem ini juga menampilkan besarnya kepercayaan kemungkinan keamanan website terancam atau tidak. Besarnya nilai kepercayaan tersebut merupakan hasil perhitungan dengan menggunakan metode Certainty Factor.	Perlu dilakukan validasi dan verifikasi yang cermat terhadap keandalan metode Certainty Factor yang digunakan. Agar metode ini sesuai untuk mengidentifikasi keamanan transaksi online pada website e-commerce dan dapat memberikan hasil yang akurat.	Perbandingan penelitian yang akan dilakukan dengan object yang berbeda dengan kepakaran yang digunakan pada audit yang sudah berkompeten, bukan merupakan asumsi peneliti.
4.	*Implementasi Algoritma Certainty Factor pada sistem pakar untuk Mendeteksi*		Membuat sebuah sistem berbasis Android untuk mendeteksi kecanduan bermain OG dengan metode	Hasil pengujian akurasi berdasarkan 18 sampel data acak yang menunjukkan nilai 83%.	Kurangnya pengetahuan yang didapat dari beberapa pakar untuk memperkuat tingkat akurasi.	Penelitian yang akan dilakukan untuk membangun sebuah sistem pakar dengan metode CF berbasis web yang dapat di akses baik lewat mobile atau desktop selain itu juga data didapatkan dari pakar langsung yaitu auditor.

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
	Kecanduan Online Games		certainty factor (CF)			
5.	*Penggunaan Metode Certainty Factor Pada Sistem Pakar Deteksi Kerusakan Perangkat Keras (Hardware) Komputer di Laboratorium Berbasis Android*		Menghasilkan sebuah sistem pakar berbasis android untuk diagnosa akhir keadaan dengan metode certainty factor yang dapat memberikan informasi mengenai 4 macam jenis diagnosa kerusakan dan 12 data gejala kerusakan	Hasil pengujian menggunakan Alpha Test terhadap 20 peserta diperoleh pilihan jawaban “Cocok” dengan nilai persentase sebesar 0,54 atau berkisar 54%.	Diperlukan pembaharuan pengetahuan dalam sistem pakar, agar dapat meningkatkan akurasi dan kemampuan deteksi kerusakan perangkat keras	Penelitian yang akan dilakukan yakni membangun sebuah sistem pakar dengan metode CF berbasis web yang dapat di akses baik lewat mobile atau desktop selain itu juga data didapatkan dari pakar langsung yaitu auditor.

2.3.Studi Pustaka

Adapun literatur yang berkaitan dengan topik penelitian ini sebagai berikut:

2.3.1.Sistem Pakar

Menurut (Pavlovic-Veselinovic, dkk, 2016) sistem pakar merujuk pada sistem komputer yang dirancang untuk meniru pengetahuan dan keahlian seorang pakar dalam domain keamanan sistem informasi. Sistem pakar ini bertujuan untuk melakukan risk assessment (penilaian risiko) terhadap keamanan sistem informasi berdasarkan standar ISO 27002.

2.3.2.Risk Assessment

Dari jurnal yang berjudul *Information security risk assessment* oleh (Kuzminykh, I., dkk, 2021) Risk Assessment merupakan proses identifikasi, analisis, dan penilaian risiko terkait keamanan sistem informasi. ISO 27002 sebagai salah satu standar internasional yang memberikan panduan tentang manajemen keamanan informasi, termasuk praktik dan prosedur yang harus diikuti untuk menjaga keamanan sistem informasi.

2.3.3.ISO 27002

Menurut (Disterer, G., 2013) ISO 27002 adalah standar internasional yang merangkum praktik keamanan informasi terbaik dalam satu kerangka kerja yang komprehensif. Standar ini memberikan pedoman untuk mengelola keamanan informasi dalam organisasi dengan mengidentifikasi, mengimplementasikan, dan memelihara kontrol keamanan yang tepat. ISO 27002 mengacu pada berbagai aspek keamanan informasi, termasuk kebijakan keamanan, pengelolaan akses, pengamanan jaringan, pengendalian operasional, serta tindakan pencegahan dan respons terhadap insiden keamanan. Dengan mengikuti ISO 27002, organisasi

dapat meningkatkan keamanan dan melindungi informasi mereka dari ancaman dan risiko yang ada. Untuk mengimplementasikan ISO 27002, maka perlu diketahui peduman kontrol yang menyediakan detail informasi untuk mendukung sebuah sistem agar dapat berjalan normal, berikut ini pedoman kontrol ISO27002:2013 (ISO/IEC 27002, 2013).

1. Information security policies
    a. Management direction for information security, yaitu kontrol untuk memberikan arahan manajemen dan dukungan untuk keamanan informasi sesuai dengan kebutuhan bisnis dan hukum dan peraturan yang relevan.
2. Organization of information security
    a. Internal organization, yaitu kontrol untuk membangun kerangka kerja manajemen untuk memulai dan mengontrol pelaksanaan dan Operasi keamanan informasi dalam organisasi.
    b. Mobile devices and teleworking, yaitu kontrol untuk menjamin keamanan teleworking dan penggunaan perangkat mobile.
3. Human resource security
    a. Prior to employment, yaitu memastikan bahwa karyawan dan kontraktor memahami tanggung jawab mereka dan cocok melakukan peran yang diterima.
    b. During employment, yaitu memastikan bahwa karyawan dan kontraktor menyadari dan memenuhi tanggung jawab keamanan informasi mereka.

c. Termination and change of employment, yaitu melindungi kepentingan organisasi sebagai bagian dari proses perubahan atau pengakhiran kerja.

4. Asset management
    a. Responsibility for assets, yaitu kontrol untuk mengidentifikasi aset organisasi dan menentukan tanggung jawab perlindungan yang tepat.
    b. Information classification, yaitu kontrol untuk memastikan kesesuaian tingkat perlindungan dengan pentingnya informasi bagi organisasi.
    c. Media handling, yaitu kontrol untuk mencegah tidak sah pengungkapan, modifikasi, penghapusan atau perusakan informasi yang tersimpan pada media.
5. Access control
    a. Business requirements of access control, yaitu untuk membatasi akses ke fasilitas pengolahan informasi dan informasi.
    b. User access management, yaitu memastikan akses pengguna yang berwenang dan untuk mencegah akses tidak sah ke sistem dan layanan.
    c. User responsibilities, yaitu kontrol untuk membuat pengguna bertanggung jawab dan menjaga informasi otentikasi mereka.
6. Cryptography
    a. Cryptographic controls, yaitu memastikan penggunaan yang tepat dan efektif kriptografi untuk melindungi kerahasiaan, keaslian dan/atau integritas informasi.
7. Physical and environmental security

a. Secure areas, yaitu mencegah akses yang tidak sah, kerusakan dan gangguan untuk informasi dan pengolahan informasi fasilitas organisasi.
b. Equipment, yaitu kontrol untuk mencegah kehilangan, kerusakan, pencurian dan gangguan pada aset operasional pada perusahaan.

8. Operations security
    a. Operational procedures and responsibilities, yaitu memastikan operasi yang benar dan aman fasilitas pengolahan informasi.
    b. Protection from malware, yaitu memastikan bahwa informasi dan informasi mengelola fasilitas dilindungi malware.
    c. Backup, yaitu melindungi data terhadap ancaman kehilangan.
    d. Logging and monitoring, yaitu merekam peristiwa dan menghasilkan bukti.
    e. Control of operational software, yaitu memastikan integritas sistem operasional.
    f. Technical vulnerability management, yaitu mencegah eksploitasi kerentanan teknis.
    g. Information systems audit considerations, yaitu kontrol untuk meminimalkan dampak dari kegiatan audit pada sistem operasi.
9. Communications security
    a. Network security management, yaitu menjamin perlindungan informasi dalam jaringan dan mendukung fasilitas pengolahan informasinya.

b. Information transfer, yaitu menjaga keamanan informasi ditransfer dalam suatu organisasi dan dengan setiap entitas eksternal.

10. System acquisition, development and maintenance
    a. Security requirements of information systems, yaitu memastikan bahwa keamanan informasi merupakan bagian integral dari sistem informasi di seluruh siklus hidup. Ini juga mencakup persyaratan untuk sistem informasi yang menyediakan layanan melalui jaringan publik.
    b. Security in development and support processes, yaitu memastikan bahwa keamanan informasi dirancang dan dilaksanakan dalam siklus hidup pengembangan sistem informasi
    c. Test data, yaitu menjamin perlindungan data yang digunakan untuk pengujian.
11. Supplier relationships
    a. Information security in supplier relationship, yaitu memastikan perlindungan aset organisasi yang dapat diakses oleh pemasok.
    b. Supplier service delivery management, yaitu menjaga tingkat disepakati keamanan informasi dan pelayanan sesuai dengan perjanjian pemasok.
12. Information security incident management
    a. Management of information security incidents and improvements, yaitu kontrol untuk memastikan konsistensi dan efektivitas pendekatan pengelolaan gangguan terkait keamanan informasi
13. Information security aspects of business continuity management

a. Information security continuity, yaitu kontrol yang terkait kontinuitas keamanan informasi harus tertanam dalam sistem manajemen kelangsungan bisnis organisasi.
b. Redundancies, yaitu kontrol untuk memastikan ketersediaan fasilitas pengolahan informasi.

14. Compliance
    a. Compliance with legal and contractual requirement, yaitu kontrol untuk menghindari pelanggaran hukum, undang-undang, peraturan atau kontrak kewajiban yang terkait dengan keamanan informasi dan persyaratan keamanan.
    b. Information security review, yaitu kontrol untuk memastikan bahwa keamanan informasi diimplementasikan dan dioperasikan sesuai dengan kebijakan dan prosedur organisasi.

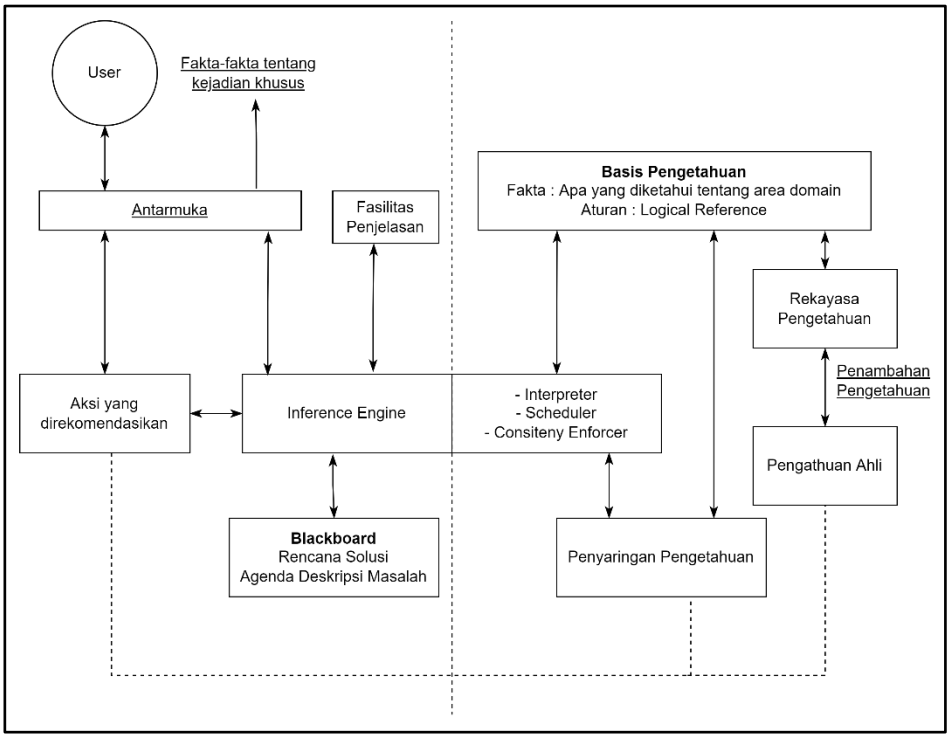
2.3.4.Certainty Factor

Menurut (Heckerman, D., 1992). *certainty factor* adalah metode yang menggunakan faktor kepastian (certainty) dalam mengukur keyakinan ahli dalam membuat penilaian. Certainty factor dapat dimanfaatkan untuk mengukur tingkat keyakinan terhadap suatu pernyataan atau hipotesis. Metode ini menggabungkan berbagai aturan atau bukti yang saling mendukung atau menentang suatu hipotesis dengan memperhitungkan faktor kepastian yang terkait. CF menggambarkan kuantitatif tingkat kepercayaan atau ketidakpercayaan terhadap suatu pernyataan, di mana angka positif menunjukkan tingkat keyakinan dan angka negatif menunjukkan tingkat ketidakpercayaan. Dengan menggunakan metode ini, sistem dapat mengambil keputusan berdasarkan bobot keyakinan yang diberikan pada

setiap pernyataan, sehingga memungkinkan analisis yang lebih terperinci dan adaptif dalam pengambilan keputusan.

2.3.5.Arsitektur Sistem Pakar

Dalam sistem pakar terdapat dua bagian pokok, yaitu lingkungan pengembangan yang digunakan sebagai pembangun komponen sistem pakar maupun basis pengetahuan dan lingkungan konsultasi yang digunakan seorang yang bukan ahli untuk melakukan konsultasi. Arsitektur sistem pakar dapat dilihat pada Gambar 2.1



Gambar 2.1 Arsitektur Sistem Pakar

Komponen yang terdapat pada Gambar 2.1 adalah sebagai berikut:

a. Antarmuka

Sebagai media komunikasi antara sistem dengan pengguna, antar muka harus dirancang dengan sederhana dan mudah dimengerti agar pengguna dapat dengan mudah untuk menjalankan sistem.

b. Sistem Penyaring Pengetahuan

Sistem ini digunakan untuk melakukan evaluasi kinerja dari sistem pakar mengenai pengetahuan yang ada, sistem akan melakukan penyaringan yang hasilnya berupa definisi pengetahuan yang dapat digunakan pada masa mendatang atau pengetahuan yang sudah tidak dapat digunakan dalam melakukan penyelesaian permasalahan.

c. Mesin Inferensi

Pada mesin inferensi terdapat metodologi yang akan digunakan untuk melakukan penalaran dan memformulasikan konklusi terhadap informasi yang terdalam dalam basis pengetahuan dan blackboard. Terdapat 3 komponen utama dalam mesin inferensi, yaitu:

1. Interpreter, bertugas untuk melakukan eksekusi terhadap item agenda yang terpilih menggunakan aturan yang terdapat pada basis pengetahuan yang sesuai.
2. Scheduler, digunakan untuk mengontrol agenda yang akan datang
3. Consistency Enforcer, digunakan untuk memelihara konsistensi dalam melakukan representasi solusi yang bersifat darurat.

d. Blackboard

Blackboard adalah area dalam memori komputer yang digunakan secara sementara untuk menyimpan kejadian yang sedang berlangsung. Blackboard juga dapat menyimpan keputusan sementara.

e. Basis Pengetahuan

Berisikan pengetahuan yang dibutuhkan dalam melakukan pemahaman terhadap masalah, melakukan formulasi, dan menyelesaikan permasalahan.

f. Fasilitas Penjelas

Merupakan komponen tambahan yang dapat meningkatkan kerja dari sistem pakar.

2.3.6.Pengujian Sistem

Pengujian sistem dalam penelitian ini terbagi menjadi dua metode, yaitu white box testing dan black box testing.

a. White box testing juga dikenal sebagai pengujian struktural, pengujian kodik, atau pengujian berbasis kodik. Metode ini melibatkan pemeriksaan internal perangkat lunak, termasuk struktur, logika, dan aliran kode. Penguji memiliki pengetahuan mendalam tentang desain dan implementasi perangkat lunak, serta akses ke kode sumbernya. Tujuan utama dari white box testing adalah untuk memastikan bahwa setiap komponen perangkat lunak bekerja dengan benar dan sesuai dengan spesifikasi. (Verma, A., dkk , 2017).

b. Black box testing juga dikenal sebagai pengujian fungsional atau pengujian berbasis spesifikasi. Metode ini memperlakukan perangkat lunak sebagai "kotak hitam" di mana penguji tidak memiliki pengetahuan tentang

implementasi internalnya. Penguji hanya berfokus pada input dan output yang diharapkan, serta perilaku perangkat lunak. (Verma, A., dkk ,2017).

2.2.7.Node.js

Node.js adalah sebuah platform yang digunakan untuk mengembangkan aplikasi berbasis web. Platform ini menggunakan JavaScript sebagai bahasa pemrogramannya. Node.js dapat menjalankan kode JavaScript di sisi server.

2.2.8.Next.js

Next.js merupakan salah satu framework React untuk membangun aplikasi web dengan menggunakan *library* React. Next.js menangani *tooling* dan konfigurasi yang dibutuhkan untuk React dan menyediakan struktur, fitur, serta optimasi tambahan untuk pengembangan aplikasi web. Next.js mendukung fitur-fitur seperti routing berbasis file-system, rendering di sisi klien dan server, data fetching dengan async/await, styling dengan berbagai metode, dan optimasi gambar, font, dan script.

2.2.9.React.js

React.js adalah sebuah library JavaScript yang bersifat open source untuk membangun user interface yang diciptakan oleh Facebook. React.js memungkinkan pengembang untuk membuat komponen UI yang interaktif dengan menggunakan syntax JSX, yang menggabungkan HTML dan JavaScript. React.js juga menggunakan DOM virtual, yaitu representasi DOM dalam memori, untuk meningkatkan performa *rendering*. React.js hanya mengurus hal-hal yang berkaitan dengan tampilan dan logika di sekitarnya, sehingga dapat digunakan bersama dengan library atau framework lain.

BAB III

LANDASAN TEORI

3.1.Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah metode deskriptif, metode ini mendeskripsikan secara rinci karakteristik sistem pakar dan proses risk assessment keamanan sistem informasi berdasarkan standar ISO 27002. Metode deskriptif memungkinkan peneliti untuk menganalisis hubungan antara variabel-variabel yang terkait, menjelaskan kriteria dan karakteristik yang digunakan, serta menyajikan temuan dengan detail. Dengan pendekatan ini, penelitian dapat memberikan pemahaman yang mendalam tentang bagaimana sistem pakar dan metode Certainty Factor dapat diterapkan dalam identifikasi dan pengelolaan risiko keamanan sistem informasi, serta memberikan rekomendasi praktis untuk meningkatkan keamanan sistem informasi berdasarkan standar ISO 27002.

3.2.Metode Pengumpulan Data

Pengumpulan data dan informasi dalam penelitian ini dilakukan dengan dua cara yaitu wawancara dan studi literatur. Wawancara dilakukan langsung kepada pakar atau auditor mengenai domain dalam ISO 27002. Sedangkan studi literatur dilakukan dengan proses mencari, mengidentifikasi, dan mengumpulkan informasi dari sumber-sumber yang sudah ada, seperti jurnal ilmiah, buku, laporan penelitian, artikel, dan dokumen lainnya yang relevan dengan topik penelitian.

3.3.Metode Pengembangan Sistem

Metode pengembangan sistem yang digunakan dalam penelitian ini adalah metode *waterfall*, metode *waterfall* adalah salah satu pendekatan tradisional dalam

pengembangan perangkat lunak yang mengikuti aliran alami dari tahap ke tahap. Pendekatan ini melibatkan urutan linier dari tahap-tahap yang terdefinisi dengan jelas, seperti analisis kebutuhan, perancangan, implementasi, pengujian, dan pemeliharaan. Setiap tahap dalam metode waterfall memiliki entri dan keluaran yang terdefinisi, dan satu tahap dimulai setelah tahap sebelumnya selesai. Pendekatan ini menekankan perencanaan yang matang sebelum memasuki tahap-tahap pengembangan berikutnya dan kurang fleksibilitas dalam merespons perubahan kebutuhan. Metode waterfall sering digunakan untuk proyek dengan kebutuhan yang stabil dan terperinci, serta ketika perubahan yang signifikan diharapkan jarang terjadi.

3.4.Metode Perancangan

Metode perancangan pada penelitian ini terbagi menjadi beberapa proses, yaitu sebagai berikut:

a. Perancangan Proses, yaitu tahapan perancangan yang menginformasikan aliran data dari masukan sampai keluaran. Perancangan proses dapat digambarkan dengan perancangan Data Flow diagram.
b. Perancangan Basis Data, yaitu proses membuat skema media penyimpanan untuk kebutuhan analisis dengan metode certainty factor. Dalam perancangan basis data berdasar dari analisis kebutuhan fungsional dan dilengkapi dengan pembuatan struktur tabel.
c. Perancangan Interface, yaitu proses merancang tampilan dan interaksi antara pengguna dengan sistem pakar yang didukung oleh kebutuhan pengguna. Interface meliputi GUI sebagai aplikasi yang menggambarkan sistem yang akan di bangun dengan menampilkan rancangan dalam bentuk

kasar yang bisa disebut dengan wireframe sebagai acuan dalam mendesain aplikasi yang akan di bangun.

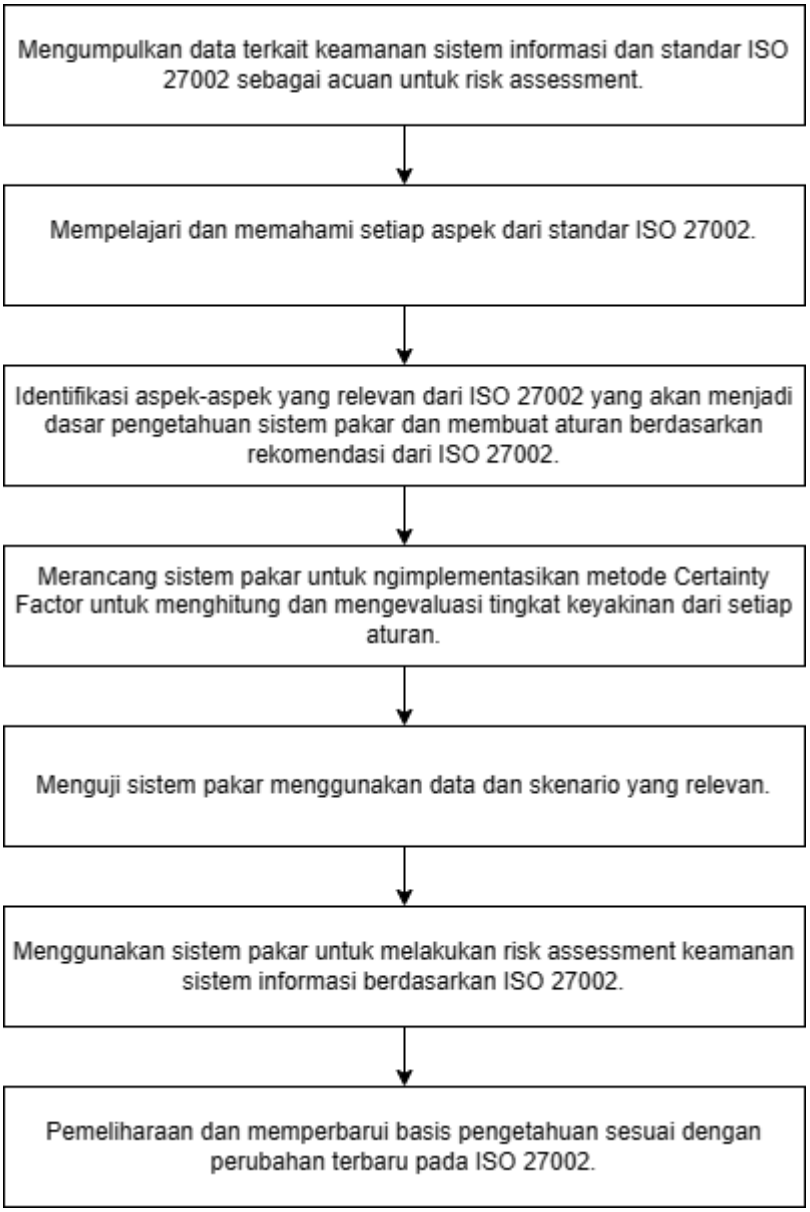
3.5.Metode Testing

Pengujian sistem merupakan tahap akhir dari proses pembuatan sistem. Pengujian sistem ini menggunakan *white box testing* dan *black box testing*. Pengujian ini bermanfaat untuk menemukan error atau bug sebagai berikut:

a. Fungsi yang tidak benar atau hilang.
b. Kesalahan interface.
c. Kesalahan kinerja.
d. Kesalahan dalam struktur data atau akses basis data eksternal.
e. Kesalahan inisialisasi dan terminasi.

3.6.Alur Proses Penelitian

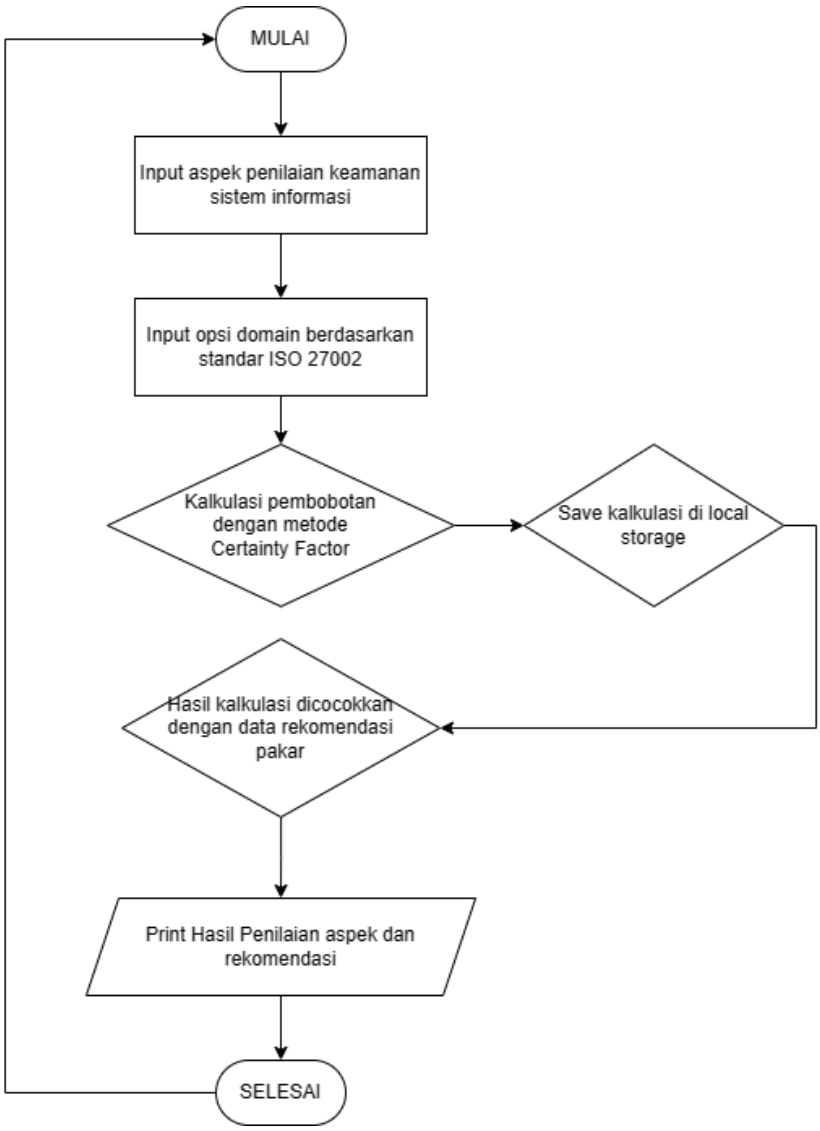
Berikut adalah alur proses penelitian yang dilakukan:



Gambar 3.1 Alur Proses Penelitian

3.7.Alur Proses Sistem Pakar

Berikut adalah alur proses sistem pakar:



Gambar 3.2 Alur Proses Sistem Pakar

RENCANA JADWAL PENELITIAN

Tabel 3.1 Rencana Jadwal Penelitian

No	Tahapan	Target Output	Bulan																							
			Maret				April				Mei				Juni				Juli				Agustus			
			1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Analisis	1. Mempelajari penelitian-penelitian terkait yang telah ada 2. Merumuskan Latar Belakang, Rumusan Masalah, Batasan Masalah, Tujuan Penelitian, Keaslian Penelitian dan Manfaat penelitian																								
2	Pengumpulan Data	Melakukan pengumpulan data yaitu dengan mencari literatur, browsing internet dan Jurnal-jurnal yang terkait dengan penelitian.																								
3	Pemodelan	Melakukan pembuatan model atau representasi yang digunakan untuk menggambarkan suatu sistem atau fenomena yang sedang diteliti.																								
4.	Pelaksanaan	Melakukan pemilihan sampel yang akan diteliti, pengumpulan data melalui observasi, pengolahan dan analisis data, serta interpretasi hasil penelitian.																								
5	Pengujian	Melakukan uji hipotesis atau teori yang telah diajukan dengan menggunakan metode ilmiah dan berbagai teknik penelitian yang telah ditentukan untuk mengumpulkan data dan menganalisis hasilnya																								
6.	Evaluasi	Mengidentifikasi kekuatan dan kelemahan dari penelitian yang dilakukan, sehingga dapat digunakan untuk meningkatkan kinerja di masa depan.																								
7.	Penarikan Kesimpulan	Menyimpulkan hasil penelitian yang telah dilakukan dengan merangkum data dan informasi yang telah dikumpulkan, serta mengevaluasi apakah tujuan penelitian telah tercapai.																								
8.	Lampiran	Melampirkan naskah utama yang berisi informasi atau data pendukung yang tidak dimasukkan ke dalam teks utama.																								

DAFTAR PUSTAKA

Aldisa, R. T. (2022). Penggunaan Metode Certainty Factor Pada Sistem Pakar Deteksi Kerusakan Perangkat Keras (Hardware) Komputer di Laboratorium Berbasis Android. *Journal of Information System Research (JOSH)*, 3(3), 314-323. https://doi.org/10.47065/josh.v3i3.1528

Andriyanto, F. (2014). Sistem pakar untuk riskassessment keamanan sistem informasi berdasarkan iso 27002 dengan metode forward chaining. https://digilib.uns.ac.id/dokumen/detail/44505

Denda, T., Wahiddin, D., & Masruriyah, A. (2022). Implementasi Algoritma Certainty Factor pada sistem pakar untuk Mendeteksi Kecanduan Online Games. *Scientific Student Journal for Information, Technology and Science*, 3(2), 160-166. http://journal.ubpkarawang.ac.id/mahasiswa/index.php/ssj/article/view/435/349

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. Journal of Information Security, 4(2). Online pada https://serwiss.bib.hs-hannover.de/frontdoor/deliver/index/docId/938/file/ISOIEC_27000_27001_and_27002_for_Information_Security_Management.pdf diakses tanggal 11 Juli 2023

Heckerman, D. (1992). The certainty-factor model. Encyclopedia of Artificial Intelligence, Second Edition, 131-138. Online pada

https://www.microsoft.com/en-us/research/publication/2016/11/The-Certainty-Factor-Model.pdf diakses tanggal 11 Juli 2023

Kuzminykh, I., Ghita, B., Sokolov, V., & Bakhshi, T. (2021). Information security risk assessment. *Encyclopedia*, 1(3), 602-617. https://www.mdpi.com/2673-8392/1/3/50

Next.js. (2023). Next.js by Vercel. Online pada https://nextjs.org diakses tanggal 12 Juli 2023

Node.js. (2023). About | Node.js. Online pada https://nodejs.org/en/about diakses tanggal 12 Juli 2023

Pavlovic-Veselinovic, S., Hedge, A., & Veselinovic, M. (2016). An ergonomic expert system for risk assessment of work-related musculo-skeletal disorders. *International Journal of Industrial Ergonomics*, 53, 130-139. https://doi.org/10.1016/j.ergon.2015.11.008

Pavlovic-Veselinovic, S., Hedge, A., & Veselinovic, M. (2016). An ergonomic expert system for risk assessment of work-related musculo-skeletal disorders. *International Journal of Industrial Ergonomics*, 53, 130-139. https://dx.doi.org/10.1016/j.ergon.2015.11.008

React.js. (2023). React. Online pada https://react.dev/ diakses tanggal 12 July 2023

Syahputra, H. (2021). Perancangan Sistem Pakar Untuk Mengidentifikasi Keamanan Transaksi Online Website E-commerce Dengan Menggunakan Metode Certainty Factor. *Informasi dan Teknologi Ilmiah (INTI)*, 8(2), 86-

89. http://stmik-budidarma.ac.id/ejurnal/index.php/inti/article/view/2899/1947

Tanuwijaya, H. (2022). Analisis Keamanan Sistem Informasi Perdagangan Terintegrasi Menggunakan Standar ISO 27002. *Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi*, 11(3), 571-582. http://dx.doi.org/10.35889/jutisi.v11i3.993

Verma, A., Khatana, A., & Chaudhary, S. (2017). A comparative study of black box testing and white box testing. *International Journal of Computer Sciences and Engineering*, 5(12), 301-304. https://studycrumb.com/alphabetizer