# PROPOSAL SKRIPSI

**SISTEM PAKAR UNTUK RISK ASSESMENT KEAMANAN SISTEM INFORMASI BERDASARKAN ISO 270002 DENGAN METODE CERTAINTY FAKTOR**



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 ASSESMENT KEAMANAN SISTEM INFORMASI BERDASARKAN ISO 270002 DENGAN METODE CERTAINTY FAKTOR**

Dipersiapkan dan Disusun oleh

**Denny Hadi Pratama**

**1912038**

Telah disetujui oleh Tim Dosen Pembimbing Skripsi  
pada tanggal, …………

Pembimbing Utama Pembimbing Pendamping

**Gunawan, S.T., M.T Wahyu Nur Alimyaningtiyas, S.Kom., M.Kom**

**NIDN 1122047201 NIDN 1103028801**

# DAFTAR ISI

[PROPOSAL SKRIPSI i](#_Toc137771566)

[HALAMAN PERSETUJUAN ii](#_Toc137771567)

[DAFTAR ISI iii](#_Toc137771568)

[DAFTAR TABEL v](#_Toc137771569)

[DAFTAR GAMBAR vi](#_Toc137771570)

[BAB I PENDAHULUAN 1](#_Toc137771571)

[1.1 Latar Belakang 1](#_Toc137771572)

[1.2 Rumusan Masalah 4](#_Toc137771573)

[1.3 Batasan Maslah 4](#_Toc137771574)

[1.4 Tujuan Penelitian 5](#_Toc137771575)

[1.5 Manfaat Penelitian 5](#_Toc137771576)

[BAB II LANDASAN TEORI 6](#_Toc137771577)

[2.1 Tinjauan Pustaka 6](#_Toc137771578)

[2.2 Penelitian Terdahulu 8](#_Toc137771579)

[2.3. Teori yang Digunakan 12](#_Toc137771580)

[2.3.1 ISO 27002 12](#_Toc137771581)

[2.3.2 Kontrol Standar ISO 27002:2013 14](#_Toc137771582)

[2.3.3 Sistem Pakar 17](#_Toc137771583)

[2.3.4 Arsitektur Sistem Pakar 19](#_Toc137771584)

[2.3.5 Certainty Factor 21](#_Toc137771585)

[2.3.6 PHP 23](#_Toc137771586)

[2.3.7 Basis Data 24](#_Toc137771587)

[2.3.8 MySQL 24](#_Toc137771588)

[BAB III METODOLOGI PENELITIAN 25](#_Toc137771589)

[3.1 Metode Penelitian 25](#_Toc137771590)

[3.2 Metode Pengumpulan Data 25](#_Toc137771591)

[3.3 Metode Pengembangan Sistem 26](#_Toc137771592)

[3.4 Metode Perancangan 27](#_Toc137771593)

[3.5 Metode Testing 28](#_Toc137771594)

[3.6 Alur Penelitian 29](#_Toc137771595)

[RENCANA JADWAL PENELITIAN 30](#_Toc137771596)

[DAFTAR PUSTAKA 31](#_Toc137771597)

# DAFTAR TABEL

[Tabel 2.1 Matriks Literatur Review dan Posisi Penelitian Judul Skripsi 9](#_Toc137770638)

[Tabel 2.2 Tingkat Keyakinan CF 21](#_Toc137770639)

# DAFTAR GAMBAR

[Gambar 2.1 Arsitektur Sistem Pakar 19](#_Toc137770951)

[Gambar 3.2 Flowchart Alur Penelitian 29](#_Toc137770953)

# BAB I PENDAHULUAN

## 1.1 Latar Belakang

Sebuah Organisasi harus menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, memelihara dan meningkatkan Sistem Manajemen Keamanan Informasi terdokumentasi dalam konteks bisnis organisasi secara keseluruhan dan risiko yang dihadapinya. Keamanan suatu sistem informasi sudah menjadi aspek yang cukup krusial dikarenakan data yang terkaji secara tidak langsung sudah bisa diakses secara publik. Dengan ada standar yang sudah ditetapkan akan dicapai suatu target organisasi yang mampu mengimplementasikan aspek keamanan sistem informasi.

Standar yang dapat digunakan dalam keamanan sebuah sistem keamanan istem informasi salah satunya adalah ISO 27000. Dalam ranah yang lebih spesifik yang terhubung secara teknis ISO 27002 merupakan pilihan yang tepat dikarenakan ruang lingkup kontrol yang ada langsung berhubungan dengan teknis bukan berupa kebijakan sehingga dapat diketahui secara langsung standar yang dirasa sudah baik, belum atau belum sama sekali diterapkan. ISO 27000 Series memberikan rekomendasi tentang information security management, risks dan controls di dalam konteks Information Security Management System (ISMS) secara keseluruhan (ISO/IEC 27002,2022). ISO 27002 merupakan Code of practice for ISMS. Terkait dengan dokumen ISO 27001, yang mana berisi panduan praktis (code of practice) teknik keamanan informasi.

Pada penerapan yang lebih lanjut banyak perusahaan besar yang memanfatkan standar ini sebagai bagian dari keamanan sistem informasi dikarenakan domain yang disediakan cukup lengkap. Penggunan ISO 27002 tentunya dibarengi dengan pengetahuan yang khusus dan disertai Auditor agar hasil yang diharapkan maksimal dan didapatkan rekomendasi yang harus dilakukan. Permasalahan yang muncul karena semakin pesatnya majunya teknologi informasi tidak hanya perusahaan skala besar yang mebutuhkan keamanan sistem informasi tapi bidang menengah atau bawah pun juga harus membutuhkannya meskipun dengan keterbatasan domain yang pokok dimiliki. Hal ini tentunya tidak sebanding dengan sumber daya yang dimiliki untuk mengadopsi ISO 27002 karena membutuhkan sumber daya yang besar. Kebutuhan dasar untuk keamanan harus diterapkan dengan bisa mengambil domaian pokok yang ada pada domain ISO 27002 seperti domain kontrol dan pengelolaan gangguan dalam keamanan sistem informasi.

Dalam perkembangan sistem informasi penggunaan pengetahuan dengan dasar dari data dan informasi sudah bisa menjadi sebuah manfaat yang dapat dirasakan langsung oleh manusia dalam kegiatan sehari hari baik untuk kepentingan pribadi atau kepentingan kemajuan perusahaan. Salah satu metode atau bidang ilmu yang dapat dimanfaatkan adalah sistem pakar. Sistem pakar merupakan cabang dari Artificial Intellegence (AI) yang cukup tua karena sistem ini mulai dikembangkan pada pertengahan 1960. Sistem pakar yang muncul pertama kali adalah General-purpose Problem Solver (GPS) yang dikembangkan oleh Newel dan Simon. Sampai saat ini banyak sistem pakar yang dibuat, seperti MYCIN untuk diagnosis penyakit, DENDRAL untuk mengidentifikasi struktur molekul campuran yang tak dikenal, XCON dan XSEL untuk membantu konfigurasi sistem komputer besar, SOPHIE untuk analisis sirkuit elektronik, Prospector digunakan di bidang geologi untuk membantu mencari dan menemukan deposit, FOLIO digunakan untuk membantu memberikan keputusan bagi seorang manajer dalam stok dan investasi, DELTA dipakai untuk pemeliharaan lokomotif listrik diesel, dan sebagainya (Sutojo, dkk., 2011).

Salah satu yang bisa dimanfaatkan dalam penggunan sistem pakar adalah metode Certainty Factor. Shortliffe Buchanan memperkenalkan Certanity Factor dalam pembuatan MYCIN pada tahun 1975 untuk mengatasi pemikiran ketidakpastian seorang ahli/pakar (Kusumadewi, 2003). Certainty Factor (CF) merupakan salah satu teknik yang digunakan untuk mengatasi ketidakpastian dalam pengambilan keputusan. Certainty Factor dapat terjadi dengan berbagai kondisi.

Dengan latar belakang tersebut yang menyoroti adanya berbagai kedalam dalam proses dalam penggunaan standar keamanan mutu keamanan sistem informasi pada berbagai perusahaan khususnya perusahaan menengah dan bawah dalam hal ini bisa dikategorikan dalam perusahaan yang sudah menerapkan sebuah sistem informasi untuk kebutuhan transaksi dan manajemen data maka perlunya sebuah standar untuk penanganan permasalahan dan pengendalian maka dalam dalam hal in bisa menggunakan iso 27002. Dari perspektif yang sudah dikemukakan maka penulis akan menyusun Tugas Akhir dengan judul “Sistem Pakar Untuk Risk Assesment Keamanan Sistem Informasi berdasarkan ISO 270002 dengan metode Certainty Faktor”**.**

## 1.2 Rumusan Masalah

Dari latar belakang yang sudah dijabarkan makan rumusan masalah dari penelitian Tugas Akhir ini sebagai berikut:

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

## 1.3 Batasan Maslah

Batasan maslaah dalam penulisan ini dimaksudkan agar pembahasan dan penulisan laporan dapat dilakukan secara terarah dan mencapai sasaran antara lain:

1. Domain yang digunakan dalam ISO 27002 adalah terdapat pada 2 aspek yaitu domain kontrol dan pengelolaan gangguan sistem informasi.
2. Hasil keluaran penelitian ini berupa sistem pakar yang digunakan untuk proses penilaian pada setiap perusahaan dengan standar ISO 27002.
3. Pengguna sistem ini dibagi kedalam 2 bagian yaitu admin yang merangkap sebagai pakar dan user pengguna umum. Sasaran user pengguna umum terdiri dari pemilik usaha yang sudah menggunakan sistem informasi berbasis transaksi dan manajemen data dalam proses bisnisnya.
4. Metode yang digunakan dalam sistem pakar menggunakan metode Certanty Factor.
5. Proses penelusuran dalam penilaian kepada pengguna menggunakan pilihan berganda dengan nilai bilangan fuzzy keyakinan.
6. Bahasa Pemrograman yang digunakan dalam membangun sistem ini menggunakan PHP dan Basis Data MySQL.
7. Pengujian yang dilakukan hanya pada sebatas pengujian sistem yang dibangun dengan fitur fitur yang sudah ada dengan metode Balckbox testing dan WhiteBox Testing.

## 1.4 Tujuan Penelitian

Adapun tujuan dari Peneltian ini sebagai berikut:

1. Membangun sebuah sistem pakar yang dapat digunakan sebagai alat untuk proses penilaian perusahaan dalam pemenuhan aspek sistem manajemen keamanan sistem informasi.
2. Memberikan informasi kepada pengguna mengenai aspek apa saja yang sekiranya dibutuhkan untuk keamanan sistem informasi.

## 1.5 Manfaat Penelitian

Adapun manfaat dari Penelitian ini sebagai berikut:

1. Menghasilkan sebuah sistem pakar yang dapat digunakan sebagai alat untuk proses penilaian perusahaan dalam pemenuhan aspek sistem manajemen keamanan sistem informasi.
2. Menambah pengetahuan informasi kepada pengguna mengenai aspek apa saja yang sekiranya dibutuhkan untuk keamanan sistem informasi.
3. Mampu memberikan alternatif bagi pengguna dalam menerpakan penggunaan ISO 27002 dalam organisasi yang ditempatinya.

# 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 ataupun penelitian terkait ISO 27002. Dalam penelitian yang dilakukan oleh Andriyanto, (2014) dalam jurnal penelitiannya dengan judul “Sistem Pakar Untuk Riskassessment Keamanan Sistem Informasi Berdasarkan Iso 27002 Dengan Metode Forward Chaining”, mempunyai tujuan Untuk membangun sebuah sistem pakar untuk mengetahui posisi atau tingkat keamananan dari sebuah perusahaan dengan melakukan risk assessment. Hasili 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 riskassessment 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 lainya yang dilakukan oleh Tanuwijaya (2022) dengan judul penlitian “Analisis Keamanan Sistem Informasi Perdagangan Terintegrasi Menggunakan Standar ISO 27002” mempunyai hasil bahwa menunjukkan pendekatan PT. XYZ terhadap keamanan Sipeter tidak konsisten dan kontrol keamanan dilakukan secara informal. Yang ditunjukan dengan maturity level Sipeter adalah 1.55 atau level Initial. Tujuan dari penelitian ini untuk menganalisis pada object untuk dilakukan analisis keamanan Sipetermenggunakan standar ISO 27002 pada klausul 8 sampai dengan klausul 14.

Syahputra, (2022) dalam jurnal penelitiannya dengan judul “Perancangan Sistem Pakar Untuk Mengidentifikasi Keamanan TransaksiOnline Website E-commerce Dengan Menggunakan Metode Certainty Factor”, menjelaskan tujuan dari penelitian ini adalah membuat sistem pakar untuk deteksi keamanan sistem informasi dengan gejala atau aturan yang ada. Hasil penelitian ini berupa Sistem Pakar ini menghasilkan keluaran berupa kemungkinan website terganggu keaamanannya atau tidak. Sistem ini juga menampilkan besarnya kepercayaan kemungkinan keamanan website terganggu atau tidak. Besarnya nilai kepercayaan tersebut merupakan hasil perhitungan dengan menggunakan metode Certainty Factor.

Dalam peneltian lainnya yang dilakukan oleh Denda, dkk (2022) dengan judul “Implementasi Algoritma Certainty Factor pada sistem pakar untuk Mendeteksi Kecanduan Online Games” mempunyai tujuan membuat sebuah sistemberbasis Android untuk mendeteksi kecanduan bermain OG dengan metode certainty factor (CF). Hasil pengujian akurasi berdasarkan 18 sampel data acak yaitu menunjukkan nilai 83%. Penelitian berikutnya dibutuhkan pengetahuan yang didapat dari beberapa pakar. Selanjutnya, penelitian berikutnya disarankan untuk menggunakan algoritma lain sebagai pembanding dalam satu sistem.

Rujukan penelitian yang kelima oleh Aldisa (20222) dengan judul yang diangkat “Penggunaan Metode Certainty Factor Pada Sistem Pakar Deteksi Kerusakan Perangkat Keras (Hardware) Komputer di Laboratorium Berbasis Android” mempunyai tujuan untuk menghasilkan sebuah sistem pakar yang berbasis android untuk diagnosa akhir keadaan menggunakan metode certainty factor dapat memberikan informasi mengenai 4 macam jenisdiagnosa kerusakan, 12 data gejala kerusakan. Hasil pengujian menggunakan Alpha Test terhadap 20 peserta diperoleh pilihan jawaban “Cocok” memiliki nilai presentase sebesar 0,54 atau seperti 54%.

## 2.2 Penelitian Terdahulu

Penelitian terdahulu mengambil dari studi kasus tentang yang berhubungan dengan standar ISO 27002 atau yang berhubungan dengan sistem pakar dengan metode Certainty Faktor. Hasil penelitian terdahulu dapat dirangkum dalam Tabel 2.1.

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 Riskassessment Keamanan Sistem Informasi Berdasarkan Iso 27002 Dengan Metode Forward Chaining* | Ferry Andriyanto  Media, Universitas Sebelas Maret Surakarta  Tahun, 2014 | Untuk membangun sebuah sistem pakar untuk mengetahui posisi atau tingkat keamananan dari sebuah perusahaan dengan melakukan risk assessment | Sistem pakar yang diusulkan memiliki tingkat kesesuaian hasil risk assessment mencapai 87,72%. Kesimpulan yang didapat adalah dengan adanya integrasi antara riskassessment 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 ini mempunyai kelemahan dengan menggunakan metode Forwar chaining dengan aturan yang ada mengharuskan pengguna mengikuti alur yang ada, jika tidak ada maka tidak akan ditemukan hailnya. | erbandingan peneltiain yang akaan dilakukan dengan metode yang berbeda yaitu akan menggunakan metode CF dengan nilai CF yang sudah di konsultasikan dengan pakar. |
| 2 | *Analisis Keamanan Sistem Informasi Perdagangan Terintegrasi Menggunakan Standar ISO 27002* | Haryanto Tanuwijaya, Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi, 2022 | Menganalisis pada object untuk dilakukan analisis keamanan Sipetermenggunakan standar ISO 27002 pada klausul 8 sampai dengan klausul 14. | Hasil penelitian menunjukkan pendekatan PT. XYZ terhadap keamanan Sipeter tidak konsisten dan kontrol keamanan dilakukan secara informal. Yang ditunjukan dengan maturity level Sipeter adalah 1.55 atau level Initial. | Pada penelitian yang dilakukan menggunakan object penelitian yang samar selain itu juga hanya sampai tahapan analisis data. | Pada peneltiian yang dilakukan akan membangun sebuah sistem pakar dengan metode certainty faktor dengan memanfaatkan domaian yang ada. |
| \3 | *Perancangan Sistem Pakar Untuk Mengidentifikasi Keamanan TransaksiOnline Website E-commerce Dengan MenggunakanMetode Certainty Factor* | Heri Syahputra, Jurnal Informasi dan Teknologi Ilmiah (INTI), 2021 | Tujuan penelitian ini adalah membuat sistem pakar untuk deteksi keamanan sistem informasi dengan gejala atau aturan yang ada. | Hasil penelitian ini berupa Sistem Pakar ini menghasilkan keluaran berupa kemungkinan website terganggu keaamanannya atau tidak. Sistem ini juga menampilkan besarnya kepercayaan kemungkinan keamanan website terganggu atau tidak. Besarnya nilai kepercayaan tersebut merupakan hasil perhitungan dengan menggunakan metode Certainty Factor. | Tidak disebutukan dalam penelitian. | Perbandingan penelitian yang akan dilakukan dengan object yang berbeda dengan kepakaran yang digunakan pada auditr yang sudah berkompeten, bukan merupakan asumsi peneliti. |
| 4 | *Implementasi Algoritma Certainty Factor pada sistem pakar untuk Mendeteksi Kecanduan Online Games* | Tri Denda, Deden Wahiddin, Anis Fitri Nur Masruriyah, Scientific Student Journal for Information, Technology and Science, 2022 | membuat sebuah sistemberbasis Android untuk mendeteksi kecanduan bermain OG dengan metode certainty factor (CF) | Hasil pengujian akurasi berdasarkan 18 sampel data acak yaitu menunjukkan nilai 83%. | penelitian berikutnya dibutuhkan pengetahuan yang didapat dari beberapa pakar. Selanjutnya, penelitian berikutnya disarankan untuk menggunakan algoritma lain sebagai pembanding dalam satu sistem | 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. |
| 5 | *Penggunaan Metode Certainty Factor Pada Sistem Pakar Deteksi Kerusakan Perangkat Keras (Hardware) Komputer di Laboratorium Berbasis Android* | Rima Tamara Aldisa  . Journal of Information System Research (JOSH), 2022 | tujuan penelitian yang dilakukan untuk menghasilkan sebuah sistem pakar yang berbasis android untuk diagnosa akhir keadaan menggunakan metode certainty factor dapat memberikan informasi mengenai 4 macam jenisdiagnosa kerusakan, 12 data gejala kerusakan | Hasil pengujian menggunakan Alpha Test terhadap 20 peserta diperoleh pilihan jawaban “Cocok” memiliki nilai  presentase sebesar 0,54 atau seperti 54%. | Tidak dijelaskan dalam peneltian | 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. |

Dari hasil penelitian terdahulu penulis akan melakukan penelitian dengan membangun sebuah sistem pakar yang dapat dimanfaatkan pelaku bisnis menengah kebawah yang tentunya cukup kesulitan dalam melaksanakan standar ISO 27002 baik dalam hal keilmuan dan biaya. Pelaku usaha di sini dibatasi bagi perusahaan yang sudah memanfaatkan teknologi dalam pengelolaan usahanya, maka dari itu penelitian ini dibatasi pada domain kontrol dan penanganan gangguan. Metode yang digunakan dalam penelitian ini menggunakan Ceratinty Faktor dengan penelusuran pertanyaan berupa pilihan ganda yang akan dijawab langsung oleh pengguna. Pengguna diharuskan terdaftar dahulu untuk dapat menggunakan sistem ini. Sistem pakar yang dibuat dengan bahasa pemrograman PHP dan basis data MySQL

## 2.3. Teori yang Digunakan

### 2.3.1 ISO 27002

ISO 27002 memberikan best practice bagi organisasi dalam mengembangkan dan mengelola standard keamanan dan bagi manajemen untuk meningkatkan keamanan informasi dalam organisasi. ISO 27002:2005 sangat berhubungan dengan 27001:2005 yaitu ISO / IEC 27001 secara resmi mendefinisikan persyaratan wajib untuk Sistem Manajemen Keamanan Informasi (SMKI) (ISO/IEC 27002, 2013). Menggunakan ISO / IEC 27002 untuk menunjukkan kontrol keamanan informasi yang sesuai dalam ISMS, tapi karena ISO / IEC 27002 hanyalah kode praktek / pedoman daripada standar sertifikasi, organisasi bebas untuk memilih dan menerapkan kontrol lain, atau memang mengadopsi alternatif suite lengkap keamanan informasi kontrol seperti yang mereka lihat cocok untuk dipakai.

Tujuan pengendalian dan kontrol dalam ISO / IEC 27002:2005 dimaksudkan untuk diterapkan untuk memenuhi persyaratan diidentifikasi oleh penilaian risiko. ISO / IEC 27002:2005 ini dimaksudkan sebagai dasar umum dan pedoman praktis untuk mengembangkan standar keamanan organisasi dan praktek manajemen keamanan yang efektif, dan untuk membantu membangun kepercayaan dalam kegiatan antar-organisasi. Banyak sistem informasi belum dirancang untuk menjadi aman. Keamanan yang dapat dicapai melalui cara-cara teknis terbatas, dan harus didukung oleh manajemen yang tepat dan prosedur.

Mengidentifikasi yang mengontrol harus di tempat membutuhkan perencanaan yang matang dan perhatian terhadap detail. Sebelum mengimplementasikan ISO 27002 perlu dilakukan penilaian risiko keamanan informasi pada suatu organisasi. ISO 27002 mengatur mengenai penilaian risiko ini. Penilaian risiko sebaiknya mengidentifikasi, menghitung dan memprioritaskan risiko terhadap kriteria untuk risiko yang bisa diterima dan tujuan yang relevan dengan organisasi. Hasil penilaian risiko sebaiknya memberikan petunjuk dan menetapkan tindakan manajemen yang tepat dan prioritas untuk mengelola risiko keamanan informasi dan untuk mengimplementasikan kontrol yang dipilih untuk melindungi terhadap risiko ini. Proses penilaian risiko dan pemilihan kontrol mungkin membutuhkan sejumlah tindakan untuk mencakup bagian sistem informasi yang berbeda-beda dari individu atau organisasi.

### 2.3.2 Kontrol Standar ISO 27002:2013

Kontrol merupakan pedoman pengimplementasian yang menyediakan detail informasi untuk mendukung sebuah sitem dapat tetap berjalan. Berikut ini merupakan kontrol yang ada pada ISO27002:2013 (ISO/IEC 27002, 2013) :

1. ***Information security policies***
2. *Management direction for information security*

Kontrol untuk memberikan arahan manajemen dan dukungan untuk keamanan informasi sesuai dengan kebutuhan bisnis dan hukum dan peraturan yang relevan.

1. ***Organization of information security***
2. *Internal organization*

Kontrol untuk membangun kerangka kerja manajemen untuk memulai dan mengontrol pelaksanaan dan Operasi keamanan informasi dalam organisasi.

1. *Mobile devices and teleworking*

Kontrol untuk menjamin keamanan teleworking dan penggunaan perangkat mobile.

1. ***Human resource security***
2. *Prior to employment*

Untuk memastikan bahwa karyawan dan kontraktor memahami tanggung jawab mereka dan cocok melakukan peran yang diterima.

1. *During employment*

Untuk memastikan bahwa karyawan dan kontraktor menyadari dan memenuhi tanggung jawab keamanan informasi mereka.

1. *Termination and change of employment*

Untuk melindungi kepentingan organisasi sebagai bagian dari prosesperubahan atau pengakhiran kerja.

1. ***Asset management***
2. *Responsibility for assets*

Kontrol untuk mengidentifikasi aset organisasi dan menentukan tanggung jawab perlindungan yang tepat.

1. *Information classification*

Kontrol untuk memastikan kesesuaian tingkat perlindungan dengan pentingnya informasi bagi organisasi.

1. *Media handling*

Kontrol untuk mencegah tidak sah pengungkapan, modifikasi, penghapusan atau perusakan informasi yang tersimpan pada media.

1. ***Access control***
2. *Business requirements of access control*

Untuk membatasi akses ke fasilitas pengolahan informasi dan informasi.

*b. User access management*

Untuk memastikan akses pengguna yang berwenang dan untuk mencegah akses tidak sah ke sistem dan layanan.

*c. User responsibilities*

Kontrol untuk membuat pengguna bertanggung jawab dan menjaga informasi otentikasi mereka.

1. ***Cryptography***
2. *Cryptographic controls*

Untuk memastikan penggunaan yang tepat dan efektif kriptografi untuk melindungi kerahasiaan, keaslian dan/atau integritas informasi.

1. ***Physical and environmental security***
2. *Secure areas*

Untuk mencegah akses yang tidak sah, kerusakan dan gangguan untuk informasi dan pengolahan informasi fasilitas organisasi.

1. *Equipment*

Kontrol untuk mencegah kehilangan, kerusakan, pencurian dan gangguan pada aset operasional pada perusahaan.

1. ***Operations security***
2. *Operational procedures and responsibilities*

Untuk memastikan operasi yang benar dan aman fasilitas pengolahan informasi.

1. *Protection from malware*

Untuk memastikan bahwa informasi dan informasi mengelola fasilitas dilindungi malware.

1. *Backup*

Untuk melindungi terhadap hilangnya data.

1. *Logging and monitoring*

Untuk merekam peristiwa dan menghasilkan bukti.

1. *Control of operational software*

Untuk memastikan integritas sistem operasional.

*f.Technical vulnerability management*

Untuk mencegah eksploitasi kerentanan teknis.

*g. Information systems audit considerations*

Kontrol untuk meminimalkan dampak dari kegiatan audit pada sistem operasi.

1. **Communications security**
2. *Network security management*

Untuk menjamin perlindungan informasi dalam jaringan dan mendukung fasilitas pengolahan informasinya.

1. *Information transfer*

Untuk menjaga keamanan informasi ditransfer dalam suatu organisasi dan dengan setiap entitas eksternal.

1. **System acquisition, development and maintenance**
2. *Security requirements of information systems*

Untuk 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.

1. *Security in development and support processes*

Untuk memastikan bahwa keamanan informasi dirancang dan dilaksanakan dalam siklus hidup pengembangan sistem informasi

1. *Test data*

Untuk menjamin perlindungan data yang digunakan untuk pengujian.

1. **Supplier relationships**
2. *Information security in supplier relationship*

Untuk memastikan perlindungan aset organisasi yang dapat diakses oleh pemasok.

1. *Supplier service delivery management*

Untuk menjaga tingkat disepakati keamanan informasi dan pelayanan sesuai dengan perjanjian pemasok.

1. **Information security incident management**
2. *Management of information security incidents and improvements*

Kontrol untuk memastikan konsistensi dan efektifitas pendekatan pengelolaan gangguan terkait keamanan informasi

1. **Information security aspects of business continuity management**
2. *Information security continuity*

Kontrol yang terkait kontinuitas keamanan informasi harus tertanam dalam sistem manajemen kelangsungan bisnis organisasi.

1. *Redundancies*

Kontrol untuk memastikan ketersediaan fasilitas pengolahan informasi.

1. **Compliance**
2. *Compliance with legal and contractual requirements*

Kontrol untuk menghindari pelanggaran hukum, undang-undang, peraturan atau kontrak kewajiban yang terkait dengan keamanan informasi dan persyaratan keamanan.

1. *Information security reviews*

Kontrol untuk memastikan bahwa keamanan informasi diimplementasikan dan dioperasikan sesuai dengan kebijakan dan prosedur organisasi.

### 2.3.3 Sistem Pakar

Sistem Pakar merupakan suatu program komputer yang mensimulasikan penilaian dan perilaku manusia atau organisasi yang memiliki pengetahuan dan pengalaman ahli dalam bidang tertentu. Biasanya sistem itu mengandung basis pengetahuan, akumulasi pengalaman dan perangkat aturan untuk menerapkan kodisi setiap suatu situasi tertentu yang dijelaskan dalam suatu program. Sistem pakar yang canggih dapat ditingkatkan dengan penambahan basis pengetahuan atau seperangkat aturan. Dengan kata lain, ini adalah sistem berbasis software yang membuat atau mengevaluasi keputusan berdasarkan aturan yang ditetapkan dalam perangkat lunak (Josephine dan Jeyabalaraja, 2012).

Dalam penyusunannya, sistem pakar mengkombinasikan kaidah-kaidah penarikan kesimpulan (inference rules) dengan basis pengetahuan tertentu yang diberikan oleh satu atau lebih pakar dalam bidang tertentu. Kombinasi dari kedua hal tersebut disimpan dalam komputer, yang selanjutnya digunakan dalam proses pengambilan keputusan untuk penyelesaian masalah tertentu.

Terdapat beberapa teknik representasi pengetahuan yang biasa digunakan dalam pengembangan suatu sistem pakar, yaitu:

1. Rule-Based Knowledge

Pengetahuan direpresentasikan dalam suatu bentuk fakta (facts) dan aturan (rules). Bentuk representasi ini terdiri atas premise dan kesimpulan

1. Frame-Based Knowledge

Pengetahuan direpresentasikan dalam suatu bentuk hirarki atau jaringan frame.

1. Object-Based Knowledge

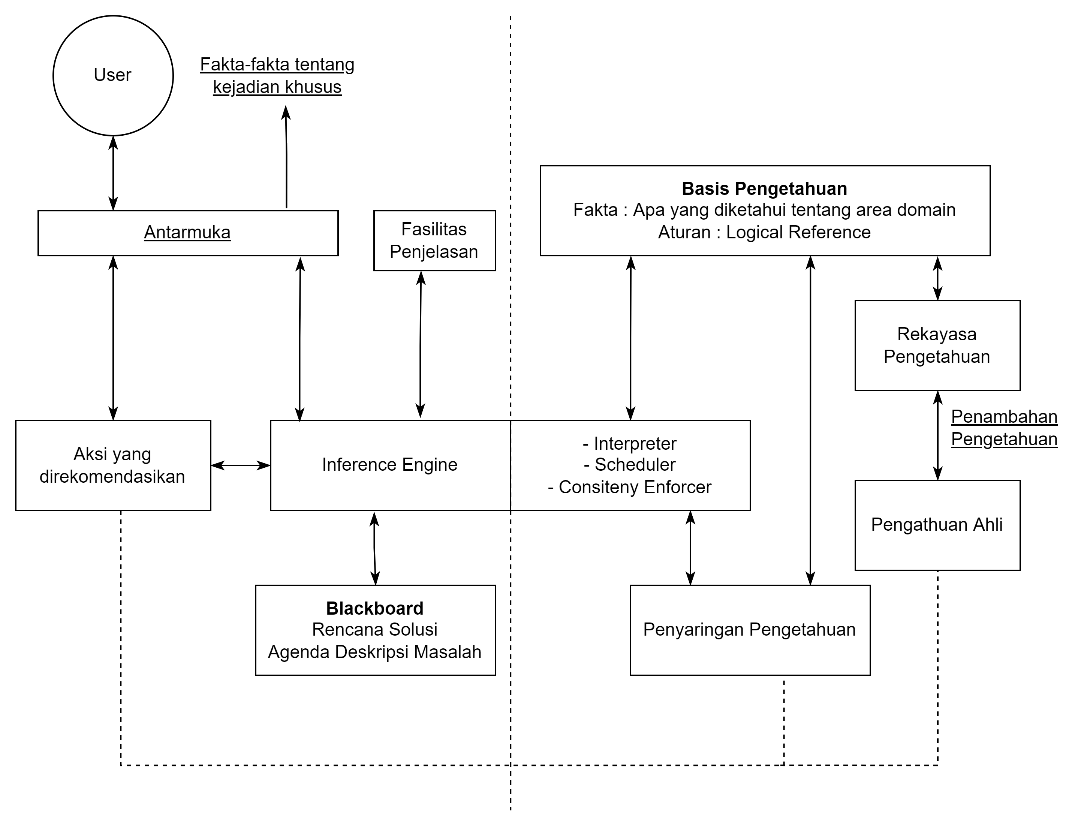
Pengetahuan direpresentasikan sebagai jaringan dari obyek-obyek. Obyek adalah elemen data yang terdiri dari data dan metoda (proses).

1. Case-Base Reasoning

Pengetahuan direpresentasikan dalam bentuk kesimpulan kasus (cases).

### 2.3.4 Arsitektur Sistem Pakar

Dalam sistem pakar terdapat 2 bagian pokok, yaitu lingkungan pengembangan yang digunakan sebagai pembangun komponen sistem pakar maupun basis pengetahuan dan lingkungan konsultasi yang digunakan untuk seorang yang bukan ahli melakukan konsultasi. Arsitektur sistem pakar dapat dilihat pada Gambar 2.1



Gambar 2.1 Arsitektur Sistem Pakar

Komponen yang ada dalam Gambar 2.1 adalah:

1. Antarmuka

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

1. Sistem Penyaring Pengetahuan

Sistem ini digunakan untuk melakukan evaluasi kinerja dari sistem pakar mengenai pengetahuan yang ada, pada sistem ini akan melakukan pengaringan yang hasilnya adalah mendefinikan pengetahuan masih cocok untuk digunakan pada masa mendatang ataukah pengetahuan sudah tidak dapat digunakan dalam melakukan penyelesaian permasalahan.

1. 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.
4. Blackboard

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

1. Basis Pengetahuan

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

1. Fasilitas Penjelas

Merupakan komponen tambahan yang dapat meningkatkan kerja dari sistem paka

### 2.3.5 Certainty Factor

Certainty theory mendasari penggunaan Certainty Factors (CFs). CFs mengekspresikan kepercayaan dalam kejadian (atau fakta atau hipotesis) berdasarkan kejadian atau penilaian seorang pakar. Sari (2013) meneliti penggunaan metode Certainty Factor (CF) dalam sistem pakar dalam mendiagnosa penyakit demam berdarah. Certainty Factor (CF) digunakan untuk menyatakan tingkat keyakinan pakar dalam suatu pernyataan (Levine, 1988). Certainty Factor dinilai dengan angka dalam rentang -1 (yakin negatif) sampai 1 (yakin positif). Pemberian nilai untuk pembagian tingkat keyakinan dapat dilihat pada **Tabel 2.1** (Intan et. Al, 2010).

Tabel 2.2 Tingkat Keyakinan CF

|  |  |
| --- | --- |
| **Kondisi Tidak Pasti (*Uncertain Term*)** | **CF** |
| Pasti Tidak (*Definetely Not*) | 0.2 |
| Hampir Pasti Tidak (*Almost Certainty Not*) | 0.3 |
| Kemungkinan Besar Tidak (*Probably Not*) | 0.4 |
| Kemungkinan Tidak (*Maybe Not*) | 0.5 |
| Tidak Tahu (*Unknown*) | 0.6 |
| Kemungkina (*Maybe*) | 0.7 |
| Kemungkinan Besar (*Probably*) | 0.8 |
| Hampir Pasti (*Almost Certainty*) | 0.9 |
| Pasti (*Definitely*) | 1.0 |

Nilai 0 menggambarkan bahwa user tidak mengalami kondisi tersebut, namun semakin tinggi nilai Cf yang dipilih maka persentasi untuk gejala tersebut juga berkemungkinan tinggi dialami user. Kemudian masing-masing aturan baru dihitung certainty factornya, sehingga diperoleh nilai certainty factor untuk masing-masing aturan, kemudian nilai certainty factor tersebut dikombinasikan.

Certainty factor menggambarkan derajat kepercayaan atau tidak kepercayaan, dimana hasil dari penjumlahan keduanya tidak selalu berjumlah 1. Certainty factor menggunakan MB(H|E) untuk menggambarkan nilai kepercayaan dari hipotesis H, Gejala E, dan MD(H|E) untuk nilai ketidakpercayaan dari hipotesis H, gejala E. Karena keterangan atau fakta bagian dari gejala salah satunya menyangkal hipotesis, MB(H|E) atau MD(H|E) maka nilainya harus nol untuk setiap H dan E. Jadi rumus untuk Certainty factor adalah sebagai berikut (Giarattano dan Riley, 1994):

 (2.1)

Dimana:

**CF (H|E)** : Certainty factor dari hipotesis H yang dipengaruhi oleh gejala (evidence) E. Besarnya CF berkisar antara -1 sampai dengan 1. Nilai -1 menunjukkan ketidakpercayaan mutlak sedangkan 1 menunjukkan kepercayaan mutlak

**MB(H|E)** : Ukuran kenaikan kepercayaan (measure of increased belief) terhadap hipotesis H yang dipengaruhi oleh gejala E

**MD(H|E)** : Ukuran kenaikan ketidakpercayaan (measure creased disbelief) terhadap hipotesis H yang dipengaruhi oleh gejala E.

**H** : Hipotesis atau dugaan penyakit

**E** : Evidence (Peristiwa atau fakta)

Certainty Factor untuk kaidah dengan kesimpulan yang serupa (Similiarly Concluded Rules) :

 (2.2)

Kelebihan dari metode ini adalah cocok digunakan pada sistem pakar yang mengukur sesuatu yang pasti atau tidak pasti seperti mendiagnosis penyakit dan perhitungan dari metode ini hanya berlaku untuk sekali hitung, serta hanya dapat mengolah dua data sehingga keakuratannya terjaga (Halim dan Hansun, 2015).

### 2.3.6 PHP

Bahasa pemrograman berbasis web yang memiliki file dengan extensi file.php dan tidak dapat diakses tanpa adanya web server adalah PHP. Menurut Hidayatullah dan Kawistara dalam bukunya yang berjudul Pemrograman Web (2017) mengemukakan bahwa “*PHP Hypertext Preprocessor* adalah suatu bahasa scripting khususnya digunakan untuk web development”. Solichin (2016), “PHP merupakan bahasa pemrograman berbasis webyang dibuat secara khusus untuk membangun aplikasi berbasis web.” Madcoms (2016),“PHP (*Hypertext preprocesso*r) adalah bahasa script yang dapat ditanamkan atau disisipkan ke dalam HTML.”

Dari beberapa definisi diatas penulis menyimpulkan bahwa PHP adalah bahasa pemograman berbasis web yang bisa kita gunakan untuk membuat aplikasi web yang disisipkan pada HTML. PHP memiliki sifat server side scripting sehingga untuk menjalankan PHP harus menggunakan web server.

### 2.3.7 Basis Data

Menurut Connolly dalam Khotijah (2016) definisi basis data adalah kumpulan data yang dihubungkan secara bersama-sama, dan gambaran dari data yang dirancang untuk memenuhi kebutuhan informasi dari suatu organisasi. Menurut Sutabri (2016) “Database adalah suatu kumpulan data terhubung (interrelated data) yang disimpan secara bersama-sama pada suatu media, tanpa mengatap satu sama lain atau tidak perlu suatu kerangkapan data (*controlled redundancy*)”.

### 2.3.8 MySQL

Menurut Madcoms (2016) “*MySQL* adalah sistem manajemen database *SQL* yang bersifat *Open Source* dan paling popular saat ini. Sistem *Database MySQL* mendukung beberapa fitur seperti *multithreaded, multi-user,* dan *SQL database management system (DBMS).* Database ini dibuat untuk keperluan sistem database yang cepat, handal, dan mudah digunakan”.

# BAB III METODOLOGI PENELITIAN

## 3.1 Metode Penelitian

Metode penelitian merupakan abstraksi dari kenyataan atau fenomena yang ada dan sedang diteliti. Dalam penelitian ini sesuai judul skripsi yang diambil ”Sistem Pakar Untuk Risk Assesment Keamanan Sistem Informasi berdasarkan ISO 270002 dengan metode Certainty Faktor”, maka model penelitian yang penulis gunakan adalah metode deskriptif.

## 3.2 Metode Pengumpulan Data

Jenis penelitian ini adalah penelitian yaitu mengembangkan sistem pakar untuk riskk Assesment dengan ISO 27002 dengan metode Certainty Factor. Pengumpulan data dan informasi dilakukan dengan 2 cara yaitu wawancara dan dokumentasi. Wawancara dilakukan langsung kepada pakar (pakar) atau auditor mengenai domaian dalam ISO 27002. Perencanaan sistem merupakan langkah awal yang dilakukan dalam penentuan tujuannya dibangun sistem. Tahap ini digunakan untuk merancang sistem pakar yang diusulkan yang meliputi daftar pertanyaan dan keputusan. Tahapan pengumpulan data dilakukan dengan cara:

1. Pengumpulan Data

Sumber data berasal dari Auditor yang berkaitan dengan ISO 27002.

1. Studi Literatur

Pada tahap ini langkah yang dilakukan setelah mengetahui pokok masalah, peneliti melakukan pencaharian, pengumpulan dan mempelajari dengan mengambil refensi yang berkaitan dengan sistem pakar dengan metode Certainty Factor. Sumber literatur berupa buku, jurnal, dan sumber-sumber yang mendukung penelitian dan perancangan system.

## 3.3 Metode Pengembangan Sistem

Model waterfall merupakan salah satu model pengembangan sistem yang sistematik dan sekuensial (Purwanto, 2019). Pada metode ini semua tahapan pengembangan harus dilakukan secara berurutan satu persatu dan berjalan secara berurutan. Berikut ini merupakan alur penelitian serta tahapan yang peneliti gunakan dalam penelitian dari metode waterfall, secara umum penelitian ini terdiri dari beberapa tahap, yaitu:

1. Tahap *requirements analysis and definition*

Pada tahap ini dilakukan pengumpulan informasi mengenai seluruh kebutuhan sistem yang akan dibangun. Informasi ini diperoleh dari hasil konsultasi dengan pengguna yang kemudian didefinisikan secara rinci dan berfungsi sebagai spesifikasi dan batasan sistem.

2. Tahap *system and software design*

Tahap perancangan sistem ini mengalokasikan kebutuhan-kebutuhan sistem yang telah diperoleh dari tahap analisis. Dalam perancangan aplikasi dibuat dengan Data Flow Diagram beserta rancangan basis data dan rancangan tampilan untuk kebutuhan pengguna.

3. Tahap *implementation and unit testing*

Dalam tahap ini dilakukan penerapan kedalam kode program, untuk penulisan kode digunakan perangkat lunak Sublime Text, Notepad ++ dan Visual Studio Code sebagai teks editor dengan menggunakan bahasa pemrograman PHP dan sesuai dengan tujuan yang diinginkan. Implementasi dimulai dari pembuatan database menggunakan MySQL sebagai manajemen basis data dan Apache sebagai web server.

4. Tahap *integration and system testing*

Tahap ini merupakan tahap pengujian sistem setelah selesai dilakukan pemrograman. Pada penelitian ini tahap testing menggunakan metode black box. Tahap ini sangat penting dilakukan sebelum diberikan ke pengguna untuk memastikan apakah sistem sudah berjalan dengan baik sesuai fungsinya.

5. Tahap *operational and maintenance*

Pada tahapan ini, sistem akan dipasang dan digunakan Politeknik Pelayaran Banten, dan selama proses penggunaannya sistem dapat dikembangan dengan menyesesuaikan fitur-fitur tambahan yang dapat menunjangan aktifitas

## 3.4 Metode Perancangan

Perancangan sistem merupakan kelanjutan dari analisis kebutuhan sistem, dimana perancangan sistem yang dibuat berdasarkan hasil analisis sistem.

1. Perancangan Proses

Merupakan tahapan perancangan yang menginformasikan aliran data dari masukan sampai keluaran. Perancangan proses dapat digambarkan dengan perancangan Data Flow diagram.

1. Perancangan Basis Data

Perancangan basis data dimaksudkan untuk 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.

1. Perancangan Interface

Perancangan antarmuka (*interface*) merupakan tahap dimana *user* atau pengguna bisa berinteraksi. Dari perancangan dan analisis sistem, yang didukung oleh kebutuhan pengguna. Beberapa perangkat lunak aplikasi 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.

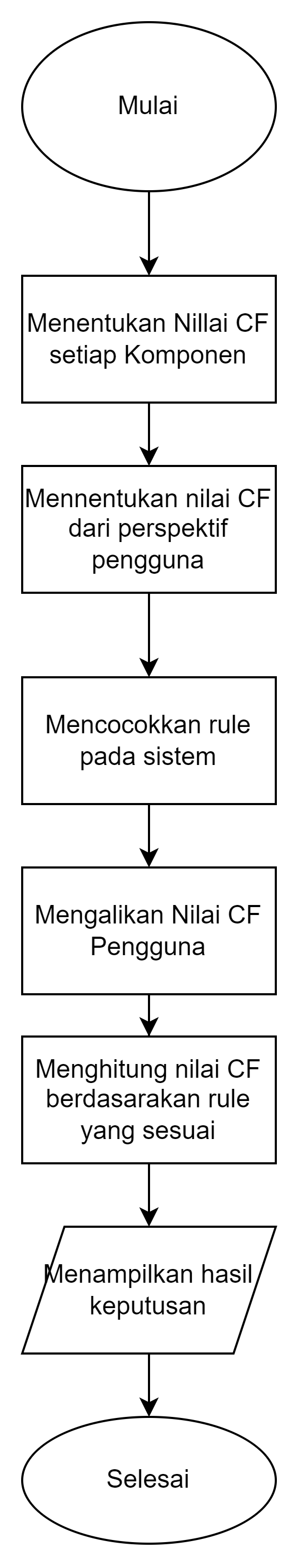
## 3.5 Metode Testing

Pengujian sistem merupakan tahap akhir dari proses pembuatan sistem. Pengujian sistem ini menggunakan *Blackbox Testing*. Menurut Pressman, Black Box Testing adalah metode pengujian yang berfokus pada persyaratan fungsional perangkat lunak. Uji coba black box memungkinkan pengembang perangkat lunak untuk menghimpun kondisi input yang akan melatih seluruh syarat-syarat fungsional suatu program. Pengujian ini berusaha menemukan kesalahan dalam kategori, sebagai berikut:

1. Fungsi yang tidak benar atau hilang.
2. Kesalahan interface.
3. Kesalahan kinerja.
4. Kesalahan dalam struktur data atau akses basis data eksternal.
5. Kesalahan inisialisasi dan terminasi.

## 3.6 Alur Penelitian

Penelitian ini akan mengembangkan sebuah sistem pakar untuk menentukan *risk assesment* keamanan sistem informasi dengan alur penelitian pada Gambar 3.1

.

Gambar 3.2 Flowchart Alur Penelitian

# RENCANA JADWAL PENELITIAN

Berisi tabel yang mengilustrasikan jadual untuk setiap tahap-tahap utama yang disebutkan dalam Jalan Penelitian disertai waktu yang dibutuhkan untuk pelaksanaan. Tabel jadwal penelitian dapat dilihat dalam Tabel 3.3.

Tabel 3.3 Rencana Jadwal Penelitian

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| No | URAIAN KEGIATAN | BULAN | | | | |
| April | Mei | Juni | Juli | Agustus |
| TAHAPAN PENYUSUNAN | | | | | | |
| 1. **Tahap Identifikasi dan Analisis** | | | | | | |
| 1 | Rumusan Masalah |  |  |  |  |  |
| 2 | Studi literatur dan studi lapangan |  |  |  |  |  |
| 1. **Tahap Pengumpulan Data** | | | | | | |
| 1 | Pengumpulan Data |  |  |  |  |  |
| 2 | Perancangan Model dan Basis Data |  |  |  |  |  |
| 1. **Tahap Perancangan Aplikasi** | | | | | | |
| 1 | Pembuatan Modul Aplikasi |  |  |  |  |  |
| 2 | Pengujian Modul Aplikasi |  |  |  |  |  |
| 3 | Deployment System |  |  |  |  |  |
| 6 | Distribusi ke *End User* |  |  |  |  |  |
| 1. **Tahap Uji Coba** | | | | | | |
| 2 | Uji Coba Fungsionalitas & Kesesuaian dengan Kebutuhan |  |  |  |  |  |
|  | | | | | | |
| 1. **Tahap Penulisan Laporan** | | | | | | |
| 1 | Proposal Penelitian |  |  |  |  |  |
| 2 | Laporan Hasil Penelitian |  |  |  |  |  |

# DAFTAR PUSTAKA

**PUSTAKA BUKU**

Hidayatullah, Priyanto, dan Jauhari, (2017). *Pemrograman WEB,* Informatika, Bandung.

Khadijah,(2016). Pengembangan Kognitif Anak Usia Dini. Medan. IKAPI.

Kusumadewi, S., (2003). Artificial Intelligence (Teknik dan Aplikasinya). Yogyakarta: Graha Ilmu.

Madcoms. (2016). Manajemen Sistem Jaringan Komputer. Yogyakarta: Andi

Purwanto. (2019). Perancangan Sistem, Informasi Pendekatan : Teori dan Praktik Siklus Akuntansi. Yogyakarta: Griya Media

Solichin, Ahmad, (2016).Pemrograman Web dengan PHP dan MySQL. Jakarta: Budi Luhur.

Sutabri, Tata,(2016). Sistem Informasi Manajemen, Andi Offset, Yogyakarta.

Sutojo, T., Edy mulyanto, Vincent, (2011). Kecerdasan Buatan, Andi Offset, Yogyakarta

**PUSTAKA MAJALAH, JURNAL ILMIAH ATAU PROSIDING**

Aldisa, Rima,. (2022). Penggunaan Metode Certainty Factor Pada Sistem Pakar Deteksi Kerusakan Perangkat Keras (Hardware) Komputer di Laboratorium Berbasis Android . Journal of Information System Research (JOSH) Volume 3, No. 3, April 2022, pp 314−323

Denda, Tri, dkk. (2022). Implementasi Algoritma Certainty Factor pada sistem pakar untuk Mendeteksi Kecanduan Online Games. Scientific Student Journal for Information, Technology and Science ISSN: 2715-2766 Vol. III No: 2, Juli 2022.

Halim, Stephanie, Seng Hansun, 2015. *Penerapan Metode Certainty Factor dalam Sistem Pakar Pendeteksi Resiko Osteoporosis dan Osteoarthritis*. ULTIMA Computing 7(2), pp.59-69, Tangerang: Universitas Multimedia Nusantara.

Josephine.M.S dan Jeyabalaraja.V (2012). Expert System and Knowledge Management for Software Developer in Software Companies. International Journal of Information and Communication Technology Research, Volume 2 No. 3, March 2012 ISSN 2223-4985

Syahputra, Heri. (2021). Perancangan Sistem Pakar Untuk Mengidentifikasi Keamanan Transaksi Online Website E-commerce Dengan Menggunakan Metode Certainty Factor. Jurnal Informasi dan Teknologi Ilmiah (INTI)Volume 8, No 2, Februari 2021

Tanuwijaya, Haryanto. (2022). Analisis Keamanan Sistem Informasi Perdagangan Terintegrasi Menggunakan Standar ISO 27002. Jutisi: Vol. 11, No. 3, Desember2022.

**PUSTAKA LAPORAN PENELITIAN**

Andriyanto,Ferry, 2014, *Sistem Pakar Untuk Riskassessment Keamanan Sistem Informasi Berdasarkan Iso 27002 Dengan Metode Forward Chaining*. Skripsi, Teknik Informatika, Univeristas Sebelas Maret, Surakarta.

Intan, Rolly & Gregorius S. Budhi, 2010. *Proposal Penerapan Probabilitas Penggunaan Fakta Guna Menentukan Certainly Factor pada Rule Base Expert System*. Surabaya : UK Petra.

**PUSTAKA ELEKTRONIK**

ISO/IEC 27002., 2013. Information Technology-Security Techniques-Code of Practice for Information Security Management ISO/IEC 17799 (27002):20013 - Final Draft. ISO/IEC JTC 1.