SKRIPSI

APLIKASI ASSESSMENT KEAMANAN SISTEM INFORMASI BERDASARKAN ISO 27002

Disusun oleh:

Nama : Denny Hadi Pratama
NIM : 1912038

PROGRAM STUDI TEKNOLOGI INFORMASI-S1
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MULIA
BALIKPAPAN

2023

SKRIPSI

APLIKASI ASSESSMENT KEAMANAN SISTEM INFORMASI BERDASARKAN ISO 27002

Diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana Komputer (S.Kom)

Disusun oleh:

Nama : Denny Hadi Pratama
NIM : 1912038

PROGRAM STUDI TEKNOLOGI INFORMASI-S1
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MULIA
BALIKPAPAN

2023

HALAMAN PENGESAHAN

APLIKASI ASSESSMENT KEAMANAN SISTEM INFORMASI BERDASARKAN ISO 27002

Dipersiapkan dan Disusun oleh

Denny Hadi Pratama

1912038

Telah Diujikan dan Dipertahankan dalam Sidang Ujian Skripsi
Program Studi S1-Teknologi Informasi
Fakultas Ilmu Komputer
Universitas Mulia Balikpapan
Pada hari Senin, 31 Juli 2023

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer

Balikpapan, 2 Agustus 2023
Dekan Fakultas Ilmu Komputer Universitas Mulia Balikpapan

Jamal, S.Kom.,M.Kom
NIDN 1102057401

HALAMAN PERSETUJUAN

APLIKASI ASSESSMENT KEAMANAN SISTEM INFORMASI BERDASARKAN ISO 27002

Dipersiapkan dan Disusun oleh

Denny Hadi Pratama

1912038

Telah Diujikan dan Dipertahankan dalam Sidang Ujian Skripsi
Program Studi S1-Teknologi Informasi
Fakultas Ilmu Komputer
Universitas Mulia Balikpapan
Pada hari Senin, 31 Juli 2023

Pembimbing Utama	**Ketua Tim Penguji**
Gunawan, S.T., M.T **NIDN 1122047201**	**Isa Rosita, S.Kom., MCs** **NIDN 1129048503**
Pembimbing Pendamping	**Anggota Tim Penguji**
Wahyu Nur Alimyaningtias, S.Kom., M.Kom **NIDN 1103028801**	**Yeyen Dwi Atma, S.Kom., M.Kom** **NIDN 1123018901**

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer

Balikpapan, 31 Juli 2023
Ketua Program Studi Teknologi Informasi

Djumhadi, S.Kom., M.Kom
NIDN 1107017101

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Denny Hadi Pratama
NIM : 1912038

Menyatakan bahwa Skripsi dengan judul berikut:
APLIKASI RISK ASSESMENT KEAMANAN SISTEM INFORMASI BERDASARKAN ISO 27002

Dosen Pembimbing Utama : Gunawan, S.T., M.T

Dosen Pembimbing Pendamping : Wahyu Nur Alimyaningtias,S.Kom.,M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas Mulia Balikpapan maupun di Perguruan Tinggi lainnya
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Tim Dosen Pembimbing
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas Mulia Balikpapan
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi

Balikpapan, 20 Juli 2023
Yang Menyatakan,

Materai Asli
Rp 6.000

Denny Hadi Pratama

HALAMAN PERSEMBAHAN

Assalamu'alaikum Warahmatullahi Wabarakatuh

Alhamdulillahirobbil'alamin, segala puji bagi Allah SWT berkat rahmat serta hidayah-Nya, tugas akhir ini dapat diselesaikan dengan lancar. Tugas akhir ini saya persembahkan untuk:

1. Untuk Ibu dan Ayah yang selalu membuatku termotivasi, selalu memberikan dukungan, selalu mendoakan, dan selalu menasehati agar menjadi pribadi yang lebih baik. Terima kasih Ibu.. Terimah kasih Ayah atas semua yang telah engkau berikan semoga diberi kesehatan dan panjang umur agar selalu dapat menemani setiap langkah kecil ku.
2. Bapak dan Ibu dosen di Universitas Mulia yang tentu saja banyak memberikan ilmunya selama proses perkuliahan.
3. Teman-teman Teknologi Informasi angkatan 2019 yang selalu memotivasi dan selalu membantu agar lulus berbarengan.
4. Tidak lupa juga saya ucapkan terima kasih kepada Google Scholarship, sebagai mesin pencari jurnal yang membuka banyak wawasan dan sumber-sumber ilmiah yang saya butuhkan selama menyusun tugas akhir ini. Serta semua pihak yang sudah membantu saya selama penyelesaian Tugas Akhir ini.

Wassalamualaikum Warahmatullahi Wabarakatuh

HALAMAN MOTTO

"Aku tidak peduli, walaupun aku harus mati untuk mengejar impianku"

-(Monkey D' Luffy)

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji syukur saya panjatkan ke hadirat Allah SWT karena atas rahmat dan karunia-Nya, skripsi ini dapat diselesaikan dengan baik. Skripsi yang berjudul "Aplikasi Risk Assessment Keamanan Sistem Informasi Berdasarkan ISO 27002" ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknologi Informasi di Universitas Mulia.

Saya ingin menyampaikan penghargaan yang setinggi-tingginya kepada bapak Gunawan, S.T., M.T dan ibu Wahyu Nur Alimyaningtias,S.Kom.,M.Kom selaku dosen pembimbing yang telah memberikan bimbingan, arahan, serta motivasi selama proses penulisan skripsi ini. Bapak Darmawan Setiya Budi, S.T., M.Kom yang banyak memberikan rekomendasi selama proses penelitian ini. Saya juga berterima kasih kepada seluruh dosen pengajar di fakultas ilmu komputer yang telah memberikan ilmu dan pengalaman yang berharga selama masa perkuliahan.

Akhir kata, saya menyadari bahwa masih banyak kekurangan dalam penyusunan skripsi ini. Oleh karena itu, saya sangat mengharapkan saran dan kritik yang membangun guna meningkatkan isi dari skripsi ini.

Wassalamualaikum Warahmatullahi Wabarakatuh

Balikpapan, 20 Juli 2023

Denny Hadi Pratama

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

ABSTRAK

Keamanan sistem informasi menjadi hal yang penting dalam era digital saat ini, di mana perusahaan dan organisasi menghadapi ancaman keamanan yang semakin kompleks dan canggih. Oleh karena itu, diperlukan pendekatan yang efektif untuk mengevaluasi risiko keamanan dalam sistem informasi.

Salah satu upaya yang dapat dilakukan adalah dengan mengembangkan sebuah Aplikasi Risk Assessment keamanan sistem informasi berdasarkan standar ISO 27002.

Aplikasi yang dikembangkan dalam penelitian ini memanfaatkan pengetahuan dan pengalaman para ahli keamanan sistem informasi yang telah ditetapkan dalam bentuk aturan-aturan berbasis ISO 27002.

Dengan menggunakan aplikasi yang dikembangkan dalam penelitian ini, organisasi dapat mengurangi kesalahan *human error* dalam proses penilaian risiko, meningkatkan akurasi penilaian risiko, dan mengoptimalkan upaya mitigasi risiko keamanan sistem informasi. Dengan demikian, Aplikasi risk assessment ini dapat menjadi alat yang berharga dalam memastikan keamanan sistem informasi yang lebih baik dan melindungi aset penting organisasi.

Kata Kunci : Aplikasi Risk Assessment, Keamanan Sistem Informasi, ISO 27002, Mitigasi Risiko, Human Error.

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, aplikasi *risk assessment* hadir sebagai solusi yang dapat membantu organisasi dalam menghadapi tantangan risk assessment keamanan sistem informasi. Dengan aturan ISO 27002, aplikasi memiliki acuan dalam pengembangan Aplikasi Risk Assessment keamanan sistem informasi.

1.2.Rumusan Masalah

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

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

1.3.Batasan Masalah

Adapun batasan masalah dalam penelitian ini sebagai berikut:

a. Hasil akhir penelitian ini berupa aplikasi web yang digunakan untuk proses penilaian pada setiap *assesment* dengan standar ISO 27002.
b. ISO 27002 sebagai acuan dalam pengembangan Aplikasi Risk Assessment keamanan sistem informasi.
c. Bahasa Pemrograman yang digunakan dalam membangun sistem ini menggunakan Node.js dan Basis Data Firebase.
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 aplikasi web 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 aplikasi 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 dokumuntasi ISO 27002 dalam proses *risk assessment*.

1.6.Keaslian Penelitian

Tabel 1.1 Matriks Literatur Review dan Posisi Penelitian

Aplikasi Assessment Keamanan Sistem Informasi Berdasarkan ISO 27002

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 acuan yang berbeda yaitu menggunakan dokementasi ISO 27002 dalam proses risk assessment.
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 aplikasi risk assessment dengan aturan-aturan ISO 27002.

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 basis pengetahuan yang digunakan pada audit yang sudah berkompeten, bukan merupakan asumsi peneliti.
4.	*Implementasi Algoritma Certainty Factor pada sistem pakar untuk Mendeteksi Kecanduan*		Membuat sebuah sistem berbasis Android untuk mendeteksi kecanduan bermain OG dengan metode certainty factor	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 aplikasi web dengan panduan ISO 27002 dan 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
	Online Games		(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 aplikasi web dengan panduan ISO 27002 berbasis web yang dapat di akses baik lewat mobile atau desktop selain itu juga data didapatkan dari pakar langsung yaitu auditor.

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.Teori-Teori yang Digunakan dalam Penelitian

Berikut adalah rangkuman teori-teori yang diambil literatur yang mendukung penelitian, serta memuat penjelasan terkait konsep dan prinsip dasar yang diperlukan untuk pemecahan permasalahan.

2.2.1.Aplikasi Web

Menurut (Taivalsaari, A, dkk, 2008) Aplikasi web adalah program perangkat lunak yang diakses dan dijalankan melalui browser web. Dalam penggunaanya, pengguna tidak perlu mengunduh atau menginstal perangkat lunak secara khusus di perangkat, melainkan dapat mengakses dan menggunakan aplikasi melalui antarmuka web yang tersedia di browser.

2.2.2.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.

2.2.3.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.

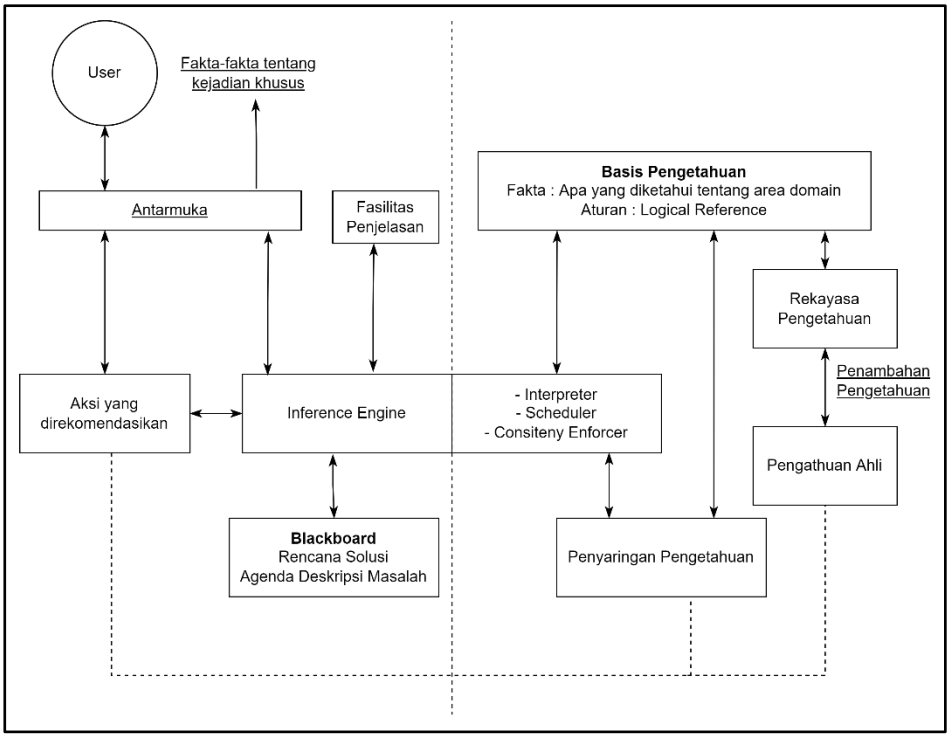
9. Communications security
   a. Network security management, yaitu menjamin perlindungan informasi dalam jaringan dan mendukung fasilitas pengolahan informasinya.
   b. Information transfer, yaitu menjaga keamanan informasi ditransfer dalam suatu organisasi dan dengan setiap entitas eksternal.
10. System 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.Arsitektur Sistem

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



Gambar 2.1 Arsitektur Sistem

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 aplikasi 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 aplikasi risk assessment.

2.2.5.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).

2.2.6.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.

2.2.7.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.

2.2.8.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

METODOLOGI PENELITIAN

3.1.Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah metode deskriptif, metode ini mendeskripsikan secara rinci karakteristik aplikasi *risk assessment* 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 aplikasi *risk assessment* dan standar ISO 27002 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*, dikutip dari (Petersen, K., Wohlin, C., & Baca, D. 2009, hal. 386-400). 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 nilai standari ISO 27002. 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 aplikasi *risk assessment* 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 pengujian *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.

3.5.1.White Box Testing

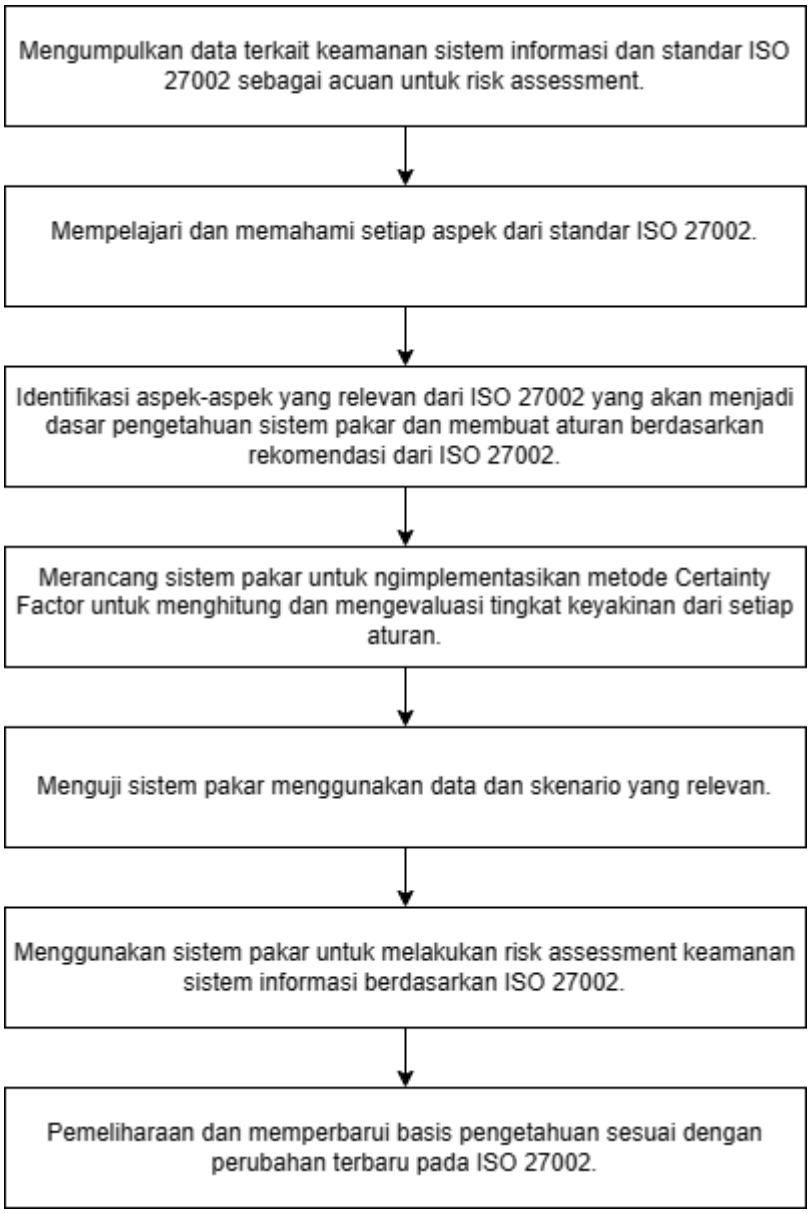
Whitebox testing dilakukan dengan memeriksa struktur internal kode perangkat lunak. Peneliti melakukan whitebox testing dengan mengakses kode sumber aplikasi dan melihat bagaimana aliran logika program berjalan. Tujuan dari pengujian *white box testing* adalah untuk menemukan kelemahan dalam algoritma, kegagalan logika, atau kode yang tidak efisien (Nidhra, S., & Dondeti, J. 2012, 29-50).

3.5.2.Black Box Testing

Adapun teknik *black box testing* yaitu melakukan pengujian tanpa pengetahuan tentang struktur internal kode perangkat lunak. Pengujian ini berfokus pada validasi fitur dan fungsionalitas perangkat lunak dari perspektif pengguna akhir. Penguji dalam blackbox testing tidak memiliki akses ke kode sumber dan harus berfokus pada spesifikasi eksternal dan persyaratan perangkat lunak (Nidhra, S., & Dondeti, J. 2012, 29-50).

3.6.Alur Proses

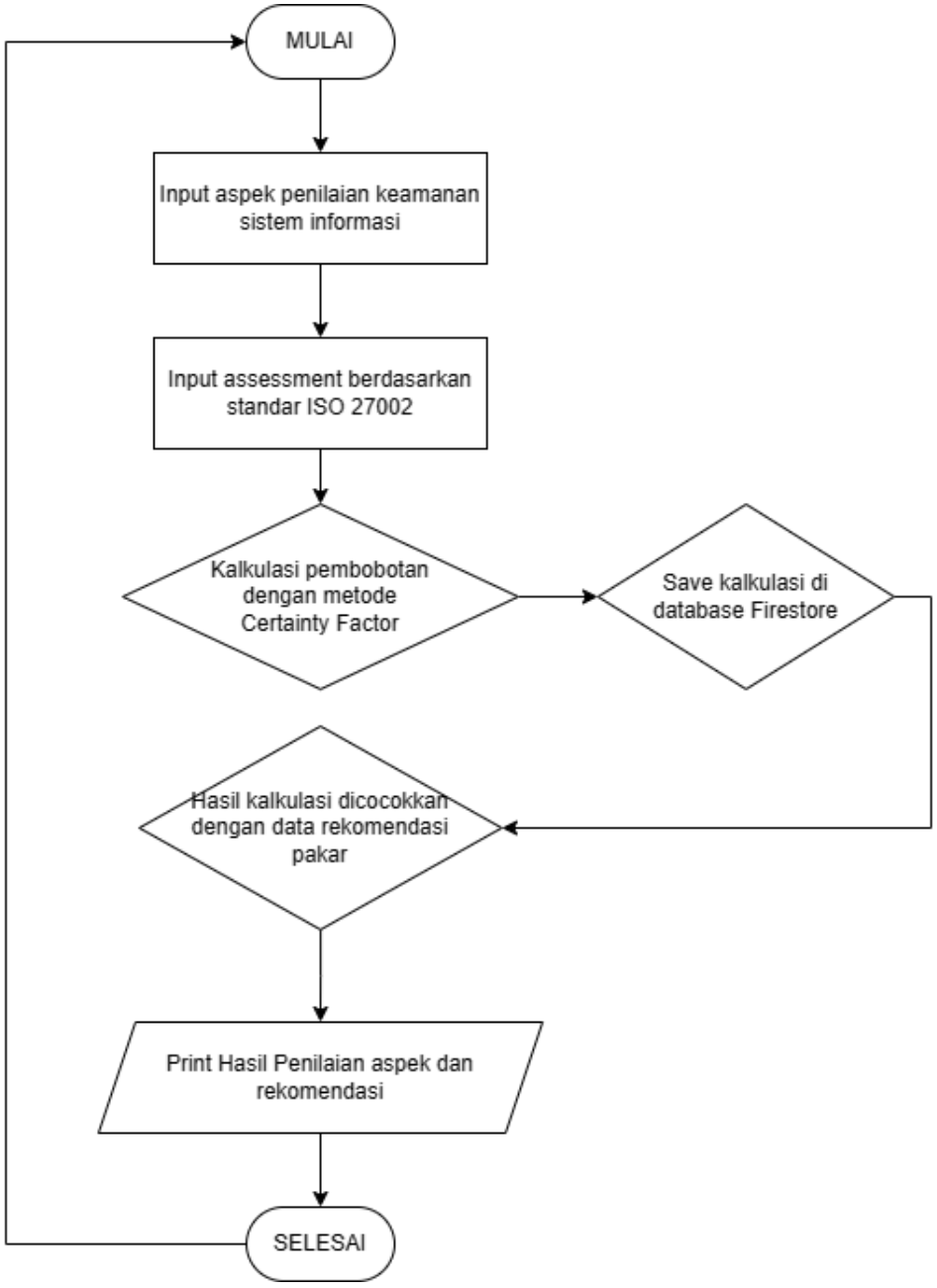
Berikut adalah alur proses penelitian yang dilakukan:



Gambar 3.1 Alur Proses Penelitian

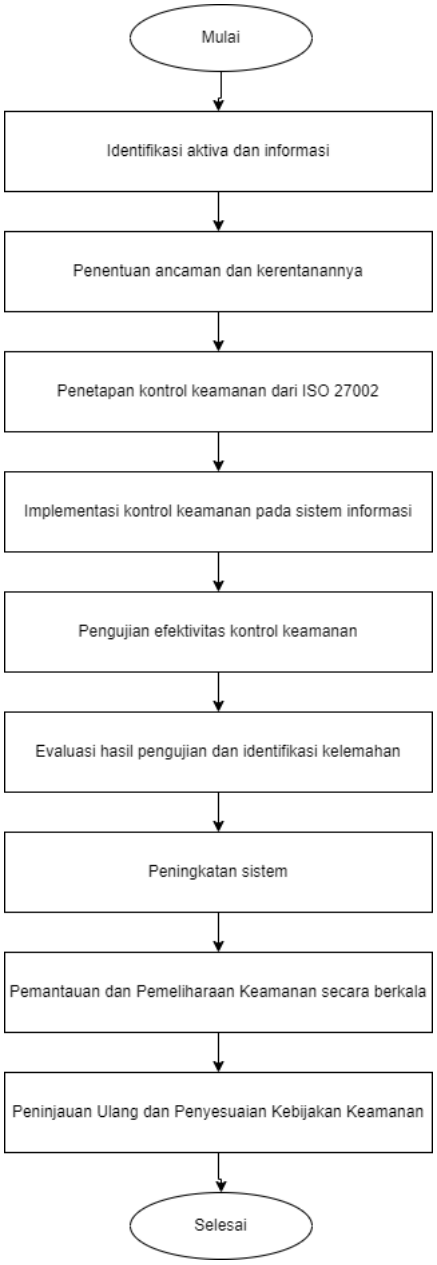
3.7.Alur Proses Aplikasi Risk Assessment

Berikut adalah alur proses aplikasi *risk assessment*:



Gambar 3.2 Alur Proses Aplikasi Risk Assessment

3.8.Flow Model Assessment



Gambar 3.3 Flow Model Assessment

BAB IV

ANALISIS DAN PERANCANGAN SISTEM

4.1.Gambaran Umum Obyek Penelitian

Penelitian ini berfokus pada pengembangan aplikasi *risk assessment* yang bertujuan untuk melakukan *risk assessment* (penilaian risiko) terhadap keamanan sistem informasi berdasarkan standar ISO 27002. ISO 27002 merupakan standar internasional yang mengatur praktik keamanan informasi dalam suatu organisasi.

Obyek penelitian ini adalah aplikasi *risk assessment* yang merupakan sebuah sistem komputer berbasis website yang memiliki pengetahuan dan kemampuan untuk memberikan rekomendasi terkait penilaian risiko keamanan sistem informasi. Aplikasi *risk assessment* ini akan menggunakan standar ISO 27002 untuk menghitung tingkat keyakinan atau kepercayaan pada suatu keputusan atau rekomendasi.

4.1.1.Domain Kontrol ISO 27002

Dalam penelitian ini, akan dikembangkan pengetahuan yang meliputi 14 domain kontrol ISO 27002, yang berpotensi sebagai kerentanan dalam sistem informasi. Pengetahuan ini akan diimplementasikan dalam *assessment* yang dapat diproses oleh aplikasi *risk assessment*.

4.1.2.Evaluasi Aplikasi *Risk Assessment*

Aplikasi *risk assessment* akan menerima masukan berupa data mengenai sistem informasi yang akan dievaluasi dari nilai *assessment*, termasuk konfigurasi, kebijakan keamanan, dan potensi ancaman lain yang mungkin terjadi. Selanjutnya, aplikasi akan menerapkan aturan-aturan berdasarkan dokumentasi

ISO 27002 untuk menghasilkan tingkat risiko keamanan sistem informasi yang diukur.

4.1.3.Output Aplikasi

Output dari aplikasi risk assessment ini berupa nilai risiko dan rekomendasi tindakan yang dapat diambil untuk mengurangi risiko atau meningkatkan keamanan sistem informasi. Rekomendasi tersebut dapat meliputi perubahan konfigurasi, penerapan kebijakan keamanan tambahan, atau tindakan lain yang diperlukan untuk mengurangi kerentanan atau memperkuat pertahanan sistem.

4.1.4.Kontrol Keamanan ISO 27002

Kontrol Keamanan ISO 27002 adalah rangkaian panduan dan praktik terstandar yang dikembangkan oleh International Organization for Standardization (ISO) untuk membantu organisasi dalam mengelola dan meningkatkan keamanan informasi. ISO 27002 adalah bagian dari keluarga standar ISO/IEC 27000 yang bertujuan untuk membantu organisasi melindungi informasi dan data sensitif mereka dari ancaman dan risiko yang mungkin terjadi.

Tabel 4.1.1 14 Kontrol Keamanan ISO 27002

No	Kontrol Keamanan	Assessment
1	Kebijakan keamanan informasi: Mengembangkan kebijakan keamanan informasi yang sesuai dengan kebutuhan organisasi.	1. Apakah organisasi telah mengembangkan kebijakan keamanan informasi yang sesuai dengan kebutuhan dan persyaratan yang dijelaskan dalam ISO 27002? 2. Bagaimana kebijakan keamanan informasi organisasi dikembangkan agar sesuai dengan karakteristik, risiko, dan kebutuhan unik organisasi? 3. Apakah kebijakan keamanan

		informasi yang telah dikembangkan oleh organisasi terkait dan sejalan dengan kebijakan lainnya yang ada? 4. Sejauh mana kebijakan keamanan informasi telah diterapkan secara konsisten di seluruh organisasi? 5. Bagaimana organisasi memantau dan mengukur kepatuhan terhadap kebijakan keamanan informasi yang telah dikembangkan? 6. Apakah dilakukan audit internal terhadap implementasi, kepatuhan, dan efektivitas kebijakan keamanan informasi? 7. Bagaimana tinjauan manajemen dilakukan untuk memastikan kebijakan keamanan informasi tetap relevan dan sesuai dengan perubahan lingkungan bisnis dan kebutuhan organisasi?
2	Organisasi keamanan informasi: Membentuk struktur organisasi yang bertanggung jawab atas keamanan informasi.	1. Apakah organisasi memiliki struktur organisasi yang ditetapkan secara jelas untuk mengelola dan bertanggung jawab atas keamanan informasi? 2. Apakah struktur organisasi keamanan informasi dirancang dan diimplementasikan dengan baik dalam organisasi? 3. Apakah peran dan tanggung jawab dalam pengelolaan keamanan informasi telah ditetapkan dengan jelas? 4. Apakah ada unit atau departemen khusus yang fokus pada keamanan informasi dan memiliki kewenangan yang memadai di dalam organisasi? 5. Apakah terdapat kolaborasi yang baik antara tim keamanan informasi dan unit lain dalam organisasi, seperti manajemen senior, departemen TI, dan bagian operasional? 6. Apakah organisasi memiliki proses

		dan mekanisme yang efektif untuk melaporkan, menangani, dan mengelola insiden keamanan informasi? 7. Apakah personel yang ditugaskan untuk mengelola keamanan informasi memiliki pengetahuan, keterampilan, dan pelatihan yang diperlukan untuk melaksanakan tugas mereka?
3	Manajemen aset: Mengelola aset informasi secara efektif, termasuk perlindungan, pemilikan, dan pemeliharaan aset.	1. Apakah organisasi memiliki proses yang ditetapkan untuk mengidentifikasi, mengklasifikasikan, dan mengelola aset informasi yang dimiliki? 2. Apakah ada kebijakan dan prosedur yang jelas untuk melindungi aset informasi organisasi, termasuk tindakan pengamanan yang tepat? 3. Apakah aset informasi organisasi telah diidentifikasi dengan jelas, termasuk kepemilikan dan tanggung jawab atas aset tersebut? 4. Apakah organisasi memiliki langkah-langkah untuk memastikan perlindungan aset informasi dari ancaman dan risiko yang ada? 5. Apakah ada prosedur yang ditetapkan untuk memelihara dan memantau kondisi serta keamanan aset informasi organisasi? 6. Apakah terdapat kebijakan atau prosedur yang mengatur pemindahan, penghapusan, atau pemusnahan aset informasi yang tidak lagi diperlukan atau relevan? 7. Apakah organisasi memiliki mekanisme untuk mendeteksi, melaporkan, dan menangani kehilangan atau penyalahgunaan aset informasi?
4	Keamanan sumber daya manusia: Memastikan bahwa karyawan memiliki kesadaran keamanan dan	1. Apakah organisasi memiliki program atau kebijakan yang secara khusus dirancang untuk

	dilibatkan dalam praktik keamanan informasi.	meningkatkan kesadaran keamanan informasi di kalangan karyawan? 2. Apakah karyawan menerima pelatihan keamanan informasi yang tepat dan berkala, termasuk penekanan pada praktik keamanan yang relevan dengan tugas dan tanggung jawab mereka? 3. Apakah terdapat kebijakan atau prosedur yang memastikan bahwa karyawan memahami dan mematuhi praktik keamanan informasi yang telah ditetapkan? 4. Apakah organisasi memiliki mekanisme untuk melibatkan karyawan dalam identifikasi, penilaian, dan pengurangan risiko keamanan informasi? 5. Apakah terdapat insentif atau penghargaan yang diberikan kepada karyawan yang berkontribusi secara positif dalam praktik keamanan informasi? 6. Apakah organisasi memiliki prosedur yang efektif untuk mengelola perubahan peran, mutasi, atau pemutusan hubungan kerja dengan karyawan dalam konteks keamanan informasi? 7. Apakah terdapat mekanisme untuk melaporkan pelanggaran keamanan informasi dan apakah karyawan merasa nyaman melaporkannya?
5	Akses kontrol: Menerapkan kontrol akses fisik dan logis untuk melindungi informasi dari akses yang tidak sah.	1. Apakah organisasi memiliki kebijakan dan prosedur yang jelas terkait dengan kontrol akses fisik dan logis untuk melindungi informasi yang dimiliki? 2. Apakah terdapat pengaturan fisik yang memadai, seperti penguncian pintu, pengawasan area terbatas, dan penggunaan kartu akses, untuk mencegah akses fisik yang tidak sah ke ruang dan fasilitas yang mengandung informasi sensitif?

		3. Apakah terdapat mekanisme untuk mengelola dan mengontrol hak akses pengguna terhadap sistem informasi yang berbasis logis? 4. Apakah prosedur autentikasi yang kuat, seperti penggunaan kata sandi yang kompleks, multi-faktor, atau biometrik, diterapkan untuk mengamankan akses logis terhadap informasi? 5. Apakah organisasi melakukan pengawasan dan pemantauan terhadap aktivitas akses fisik dan logis untuk mendeteksi dan mengatasi upaya akses yang tidak sah? 6. Apakah ada kebijakan dan prosedur yang ditetapkan untuk mengelola perubahan terkait hak akses fisik dan logis, termasuk pengangkatan hak akses yang tidak lagi diperlukan? 7. Apakah organisasi memiliki proses untuk melakukan audit terhadap kontrol akses fisik dan logis secara berkala guna memastikan kepatuhan dan keefektifan implementasinya?
6	Perencanaan dan pemulihan bencana: Mengembangkan dan mengimplementasikan rencana pemulihan bencana yang memadai untuk mengatasi gangguan layanan	1. Apakah organisasi telah mengembangkan rencana pemulihan bencana yang memadai untuk mengatasi gangguan layanan yang mungkin terjadi? 2. Apakah proses identifikasi risiko dan analisis dampak telah dilakukan untuk menyusun rencana pemulihan bencana yang tepat dan relevan? 3. Apakah rencana pemulihan bencana mencakup langkah-langkah yang jelas untuk memulihkan layanan dengan cepat dan efisien setelah terjadinya gangguan? 4. Apakah ada mekanisme untuk menguji dan melatih rencana pemulihan bencana secara berkala guna memastikan keandalan dan

		kesiapan saat diimplementasikan? 5. Apakah rencana pemulihan bencana diperbarui secara teratur sesuai dengan perubahan yang terjadi dalam infrastruktur teknologi dan kebutuhan organisasi? 6. Apakah peran dan tanggung jawab individu atau tim yang bertanggung jawab dalam pelaksanaan rencana pemulihan bencana telah ditetapkan dengan jelas? 7. Apakah ada mekanisme pelaporan dan evaluasi setelah terjadinya gangguan yang memungkinkan organisasi untuk mengidentifikasi pelajaran dan melakukan perbaikan berkelanjutan pada rencana pemulihan bencana?
7	Manajemen keamanan operasional: Memastikan operasi keamanan yang efektif melalui pemantauan, pemeliharaan, dan perlindungan sistem.	1. Apakah organisasi memiliki proses pemantauan yang efektif untuk mengawasi operasi keamanan dan mendeteksi potensi ancaman atau pelanggaran keamanan? 2. Apakah ada jadwal dan prosedur pemeliharaan yang ditetapkan untuk memastikan keberlanjutan dan kinerja optimal sistem keamanan? 3. Apakah sistem keamanan organisasi dilindungi secara memadai dari serangan dan gangguan dengan menggunakan teknologi dan solusi keamanan yang sesuai? 4. Apakah telah ditetapkan kebijakan dan prosedur untuk menjaga kerahasiaan, integritas, dan ketersediaan data dan sistem? 5. Apakah organisasi memiliki prosedur pemulihan bencana yang memadai untuk mengatasi kerusakan atau gangguan yang dapat terjadi pada sistem keamanan operasional? 6. Apakah dilakukan penilaian risiko secara berkala terhadap sistem keamanan operasional guna

		mengidentifikasi ancaman baru dan memastikan langkah-langkah perlindungan yang relevan? 7. Apakah organisasi memiliki mekanisme pelaporan dan penanganan insiden yang efektif untuk mengatasi dan merespons kejadian keamanan yang mungkin terjadi?
8	Keamanan komunikasi dan operasi: Melindungi informasi saat diproses, disimpan, dan ditransmisikan.	1. Apakah ada kebijakan dan prosedur yang telah ditetapkan untuk melindungi informasi saat diproses, disimpan, dan ditransmisikan? 2. Apakah dilakukan enkripsi untuk melindungi kerahasiaan dan integritas informasi yang diproses, disimpan, atau ditransmisikan melalui jaringan atau media lainnya? 3. Apakah ada mekanisme pengelolaan kunci yang aman untuk mendukung implementasi enkripsi dan menghindari penggunaan kunci yang lemah atau tidak aman? 4. Apakah terdapat pemantauan dan pengendalian yang efektif untuk melindungi informasi saat diproses, seperti kontrol akses, pemisahan tugas, dan pembatasan hak akses? 5. Apakah langkah-langkah keamanan teknis telah diimplementasikan untuk melindungi informasi saat disimpan, seperti penggunaan firewall, antivirus, dan mekanisme keamanan lainnya? 6. Apakah ada kebijakan dan prosedur yang mengatur penggunaan perangkat seluler, perangkat USB, dan media penyimpanan lainnya untuk mencegah kebocoran atau penyalahgunaan informasi? 7. Apakah ada langkah-langkah perlindungan yang efektif untuk melindungi informasi saat ditransmisikan melalui jaringan,

		seperti penggunaan VPN, protokol keamanan, atau tautan aman?
9	Pengendalian akses sistem informasi: Menerapkan kontrol untuk mencegah akses yang tidak sah atau tidak pantas ke sistem informasi.	1. Apakah ada kebijakan dan prosedur yang jelas untuk mengelola akses ke sistem informasi? 2. Apakah kebijakan dan prosedur tersebut dikomunikasikan kepada semua pengguna sistem informasi? 3. Apakah ada proses untuk memverifikasi identitas pengguna sebelum mereka diberikan akses ke sistem informasi? 4. Apakah ada proses untuk membatasi akses pengguna ke data dan sistem yang mereka butuhkan untuk melakukan pekerjaan mereka? 5. Apakah ada proses untuk melacak akses pengguna ke sistem informasi dan data? 6. Apakah ada proses untuk menanggapi akses yang tidak sah atau tidak pantas ke sistem informasi? 7. Apakah ada proses untuk memulihkan sistem informasi dari akses yang tidak sah atau tidak pantas?
10	Perolehan, pengembangan, dan pemeliharaan sistem informasi: Memastikan bahwa keamanan diintegrasikan dalam siklus hidup pengembangan sistem informasi.	1. Apakah ada kebijakan dan prosedur yang jelas untuk integrasi keamanan dalam siklus hidup pengembangan sistem informasi? 2. Apakah kebijakan dan prosedur tersebut dikomunikasikan kepada semua pihak yang terlibat dalam pengembangan sistem informasi? 3. Apakah ada proses untuk mengidentifikasi dan mengevaluasi risiko keamanan pada sistem informasi yang sedang dikembangkan? 4. Apakah ada proses untuk mengurangi risiko keamanan pada sistem informasi yang sedang

		dikembangkan? 5. Apakah ada proses untuk menguji keamanan sistem informasi yang sedang dikembangkan? 6. Apakah ada proses untuk mendokumentasikan keamanan sistem informasi yang sedang dikembangkan? 7. Apakah ada proses untuk memelihara keamanan sistem informasi yang telah dikembangkan?
11	Pengelolaan ketidaksesuaian: Mengelola insiden keamanan dan pelanggaran keamanan yang terjadi.	1. Apakah organisasi memiliki kebijakan dan prosedur yang ditetapkan untuk mengelola insiden keamanan dan pelanggaran keamanan yang terjadi? 2. Apakah terdapat mekanisme pelaporan yang efektif untuk melaporkan insiden keamanan dan pelanggaran keamanan kepada pihak yang berwenang? 3. Apakah organisasi memiliki tim atau personil yang ditugaskan secara khusus untuk menangani dan merespons insiden keamanan dengan cepat dan efektif? 4. Apakah ada proses investigasi yang ditetapkan untuk menganalisis penyebab dan dampak insiden keamanan serta untuk mengambil tindakan yang sesuai? 5. Apakah dilakukan dokumentasi dan pelaporan yang tepat terkait dengan insiden keamanan dan langkah-langkah yang diambil untuk menanganinya? 6. Apakah organisasi melakukan pelatihan dan kesadaran kepada karyawan terkait dengan pelaporan insiden keamanan dan pentingnya kerjasama dalam penanganannya? 7. Apakah terdapat prosedur pemulihan setelah terjadinya insiden keamanan untuk

		mengembalikan sistem dan data ke keadaan yang aman dan operasional?
12	Aspek keamanan pada hubungan bisnis: Menjaga keamanan informasi saat menjalin hubungan bisnis dengan pihak eksternal.	1. Apakah organisasi memiliki kebijakan dan prosedur yang mengatur keamanan informasi saat menjalin hubungan bisnis dengan pihak eksternal? 2. Apakah dilakukan evaluasi risiko terkait dengan hubungan bisnis dengan pihak eksternal untuk memastikan perlindungan informasi dan kepatuhan terhadap standar keamanan yang berlaku? 3. Apakah terdapat perjanjian kerahasiaan atau kontrak keamanan yang ditetapkan dengan pihak eksternal untuk melindungi informasi rahasia atau sensitif? 4. Apakah ada mekanisme pengawasan dan pemantauan yang efektif untuk mengontrol akses dan penggunaan informasi oleh pihak eksternal? 5. Apakah terdapat proses pengendalian untuk memastikan bahwa informasi yang dibagikan kepada pihak eksternal hanya sesuai dengan kebutuhan bisnis dan sesuai dengan tingkat keamanan yang telah ditentukan? 6. Apakah dilakukan pemantauan terhadap kepatuhan pihak eksternal terhadap persyaratan keamanan informasi yang telah ditetapkan? 7. Apakah organisasi memiliki mekanisme untuk menangani pelanggaran keamanan yang dilakukan oleh pihak eksternal dan mengambil tindakan yang sesuai?
13	Kepatuhan terhadap standar: Memastikan kepatuhan dengan persyaratan hukum, regulasi, dan standar industri yang berlaku.	1. Apakah organisasi memiliki proses yang ditetapkan untuk memastikan kepatuhan terhadap persyaratan hukum yang berlaku terkait dengan

		keamanan informasi? 2. Apakah dilakukan evaluasi terhadap regulasi dan persyaratan industri yang berlaku untuk memastikan kepatuhan dan implementasi yang tepat? 3. Apakah ada tim atau personil yang ditugaskan secara khusus untuk memantau dan mengelola kepatuhan terhadap persyaratan hukum, regulasi, dan standar industri yang relevan? 4. Apakah terdapat kebijakan dan prosedur yang telah ditetapkan untuk mengelola perubahan dalam persyaratan hukum atau regulasi terkait keamanan informasi? 5. Apakah dilakukan audit internal secara berkala untuk mengevaluasi tingkat kepatuhan organisasi terhadap persyaratan hukum, regulasi, dan standar industri yang berlaku? 6. Apakah terdapat proses pelaporan yang efektif untuk melaporkan pelanggaran hukum, regulasi, atau persyaratan industri terkait keamanan informasi? 7. Apakah organisasi memiliki mekanisme pemantauan dan peninjauan yang sistematis untuk memastikan bahwa kepatuhan dengan persyaratan hukum dan regulasi terus dipatuhi?
14	Audit keamanan informasi: Melakukan audit secara teratur untuk mengevaluasi efektivitas kontrol keamanan informasi.	1. Apakah organisasi melakukan audit keamanan informasi secara teratur untuk mengevaluasi efektivitas kontrol keamanan yang telah diimplementasikan? 2. Apakah dilakukan penjadwalan audit keamanan informasi yang mencakup seluruh aspek sistem dan kebijakan keamanan yang ada? 3. Apakah ada tim atau personel yang bertanggung jawab secara khusus

		dalam melaksanakan audit keamanan informasi di organisasi? 4. Apakah terdapat metode dan prosedur audit yang telah ditetapkan untuk memastikan konsistensi dan obyektivitas dalam pelaksanaan audit keamanan informasi? 5. Apakah hasil dari audit keamanan informasi dikomunikasikan secara efektif kepada pihak yang berwenang dan pihak-pihak yang terkait? 6. Apakah organisasi telah mengambil langkah-langkah untuk menindaklanjuti rekomendasi atau temuan dari audit keamanan informasi yang telah dilakukan sebelumnya? 7. Apakah dilakukan pemantauan dan pengukuran terhadap tindak lanjut yang diambil sebagai hasil dari audit keamanan informasi untuk memastikan implementasi yang efektif?

Pada tabel, merupakan kumpulan kontrol dan assessment yang akan diimplementasikan kedalam aplikasi *risk assessment* untuk menganalisis tingkat keamanan sebuah organisasi dalam menghadapi berbagai ancaman keamanan informasi, termasuk serangan siber, pencurian data, dan pelanggaran keamanan lainnya.

Untuk menentukan rentang nilai ISO 27002, maka harus diketahui nilai tertinggi assessment, assessment pada aplikasi *risk assessment* ini terdiri dari 14 domain, 7 assessment masing-masing domian dengan bobot tertinggi adalah 3. Maka rumus yang digunakan adalah sebagai berikut:

“rentang tertinggi = (kontrol keamanan x jumlah assessment) x nilai assessment tertinggi "

(14 x 7) x 3 = 294

Maka nilai tertinggi yang didapat adalah 294.

Tabel 4.1.2 Rentang Nilai ISO 27002

Skor Total	Kategori
0-50	Risiko Tinggi
51-99	Risiko Sedang
100-199	Risiko Rendah
200-294	Risiko Sangat Rendah

Pada Tabel 4.1.2, merupakan rentang nilai dari keseluruhan assessment, nilai tertinggi adalah rentang 200-294 yang berarti memiliki risiko keamanan yang rendah. Penetapan rentang nilai ISO 27002 untuk kategori risiko ini merupakan hasil dari konsensus dan pengalaman pakar (Darmawan Setiya Budi, S.T., M.Kom) yang terlibat dalam proses penilaian risiko serta pertimbangan dari kerangka kerja ISO 27002.

Tabel 4.1.3 Rentang Nilai Aspek Tiap Kontrol

Skor Nilai Aspek	Nilai
0	Tidak Layak
1-7	Memenuhi Kerangka Dasar
8-15	Cukup Baik
16-21	Baik

Pada Tabel 4.1.2, merupakan rentang untuk nilai dari tiap kontrol keamanan, tiap kontrol keamanan berisi 7 assessment dengan nilai paling tinggi adalah 21 dan rentang nilai yang baik adalah 16-21.

Selanjutnya adalah umpan balik dari 14 kontrol keamanan sistem informasi.

Tabel 4.1.4 Umpan Balik Kebijakan Keamanan Informasi

Nilai	Umpan Balik
Tidak Layak	Kontrol keamanan informasi ini tidak memenuhi standar ISO 27002 dan menghadirkan risiko serius bagi organisasi. Organisasi perlu melakukan evaluasi mendalam dan memperbaiki kontrol ini untuk memastikan kepatuhan dan perlindungan yang lebih baik terhadap informasi.
Memenuhi Kerangka Dasar	Kontrol ini memenuhi beberapa elemen dasar dari ISO 27002, tetapi masih memerlukan banyak perbaikan untuk mencapai tingkat kepatuhan yang lebih baik. Organisasi perlu mengidentifikasi area yang perlu diperbaiki dan meningkatkan detail serta ketepatan kebijakan.
Cukup Baik	Kontrol keamanan informasi ini cukup memenuhi persyaratan dasar ISO 27002 dan mencakup banyak elemen yang diperlukan. Organisasi perlu melakukan evaluasi rutin dan memperbaiki kebijakan sesuai dengan perubahan lingkungan dan ancaman keamanan.
Baik	Kontrol keamanan informasi ini sepenuhnya mematuhi standar ISO 27002 dan menunjukkan keunggulan dalam penerapan kebijakan keamanan informasi.

Tabel 4.1.5 Umpan Balik Organisasi Keamanan Informasi

Nilai	Umpan Balik
Tidak Layak	Kontrol ini belum diterapkan atau diterapkan secara sangat tidak memadai dalam organisasi keamanan informasi. Kekurangan dalam implementasi dapat menyebabkan risiko keamanan yang tinggi dan rentan terhadap ancaman internal dan eksternal.
Memenuhi Kerangka	Kontrol ini telah diimplementasikan secara dasar, namun ada beberapa kelemahan atau celah keamanan yang perlu diperbaiki.

Dasar	Implementasi kontrol ini mungkin belum konsisten dan tidak sepenuhnya mengikuti panduan yang ditetapkan oleh ISO 27002.
Cukup Baik	Kontrol ini telah diimplementasikan dengan baik dan sebagian besar aspek keamanannya telah diterapkan secara memadai. Namun, mungkin masih ada beberapa area yang dapat ditingkatkan untuk meningkatkan keamanan secara keseluruhan.
Baik	Kontrol ini telah diimplementasikan dengan sangat baik dan mencapai standar keamanan informasi yang diinginkan sesuai dengan ISO 27002.

Tabel 4.1.6 Umpan Balik Manajemen Aset

Nilai	Umpan Balik
Tidak Layak	Kontrol keamanan ini tidak dipatuhi atau diabaikan sepenuhnya. Risiko kehilangan, kebocoran, atau penyalahgunaan aset informasi sangat tinggi, dan organisasi tidak mengambil tindakan yang memadai untuk mengatasi masalah ini.
Memenuhi Kerangka Dasar	Organisasi memiliki kerangka dasar untuk mengelola aset informasi, namun implementasinya masih terbatas. Beberapa aset mungkin sudah terlindungi, tetapi masih ada area yang rentan dan memerlukan perhatian lebih.
Cukup Baik	Kontrol keamanan ini telah diimplementasikan dengan cukup baik oleh organisasi. Organisasi juga telah melaksanakan tindakan pemeliharaan rutin untuk memastikan aset tetap relevan dan aman dari ancaman yang mungkin timbul.
Baik	Organisasi telah mencapai tingkat keunggulan dalam mengelola aset informasi.

Tabel 4.1.7 Umpan Balik Keamanan Sumber Daya Manusia

Nilai	Umpan Balik
Tidak Layak	Tidak ada upaya untuk memberikan pelatihan dan kesadaran keamanan yang memadai kepada karyawan.
Memenuhi Kerangka Dasar	Sebagian besar karyawan memiliki kesadaran tentang pentingnya keamanan informasi dan terlibat dalam beberapa praktik keamanan. Meskipun ada kesadaran, keterlibatan aktif dalam

	mengidentifikasi dan melaporkan insiden keamanan masih perlu ditingkatkan.
Cukup Baik	Karyawan secara umum memiliki pemahaman yang baik tentang pentingnya keamanan informasi dan terlibat secara aktif dalam praktik keamanan. Karyawan cenderung melaporkan insiden keamanan dan bekerja sama dalam mengidentifikasi dan mengurangi risiko keamanan.
Baik	Karyawan memiliki kesadaran yang tinggi tentang pentingnya keamanan informasi dan secara proaktif terlibat dalam menjalankan praktik keamanan.

Tabel 4.1.8 Umpan Balik Akses Kontrol

Nilai	Umpan Balik
Tidak Layak	Kontrol keamanan ini tidak diimplementasikan atau diabaikan sepenuhnya. Tidak ada upaya yang dilakukan untuk melindungi informasi dari akses yang tidak sah, baik secara fisik maupun logis. Kondisi ini meningkatkan risiko kebocoran data dan potensi kehilangan informasi yang sangat sensitif.
Memenuhi Kerangka Dasar	Kontrol keamanan ini ada, tetapi implementasinya masih sangat terbatas dan belum sepenuhnya sesuai dengan standar ISO 27002. Beberapa upaya telah dilakukan untuk menerapkan kontrol akses fisik dan logis, namun masih ada kelemahan dan celah yang dapat dieksploitasi oleh pihak yang tidak sah.
Cukup Baik	Penerapan kontrol akses fisik dan logis telah mencapai tingkat yang cukup baik sesuai dengan ISO 27002. Upaya yang serius telah dilakukan untuk melindungi informasi dari akses yang tidak sah. Namun, masih ada beberapa area yang perlu ditingkatkan untuk mencapai tingkat keamanan yang optimal.
Baik	Kontrol keamanan ini diimplementasikan dengan sangat baik sesuai dengan standar ISO 27002. Semua persyaratan untuk menerapkan kontrol akses fisik dan logis telah dipenuhi dengan benar. Informasi sensitif dan kritis telah terlindungi dengan efektif dari akses yang tidak sah, baik dari segi fisik maupun logis. Sistem keamanan ini dianggap kuat dan handal.

Tabel 4.1.9 Umpan Balik Perencanaan dan Pemulihan Bencana

Nilai	Umpan Balik
Tidak Layak	Organisasi ini tidak memiliki rencana pemulihan bencana yang jelas dan terstruktur untuk mengatasi gangguan layanan. Kurangnya perencanaan ini dapat menyebabkan ketidakmampuan untuk memulihkan layanan dengan efisien, menyebabkan kerugian yang signifikan bagi bisnis dan pelanggan.
Memenuhi Kerangka Dasar	Organisasi ini telah mengambil langkah awal dalam mengembangkan rencana pemulihan bencana. Mereka telah mengidentifikasi beberapa risiko potensial dan mulai menyusun rencana dasar untuk mengatasi gangguan layanan. Namun, rencana ini mungkin masih perlu diperbaiki dan diperinci agar lebih efektif.
Cukup Baik	Organisasi ini telah berhasil mengembangkan dan mengimplementasikan rencana pemulihan bencana yang memadai. Rencana pemulihan ini juga telah diuji secara berkala dan telah melibatkan seluruh tim terkait. Meskipun ada ruang untuk peningkatan dan perbaikan, rencana pemulihan ini memberikan fondasi yang solid untuk menghadapi bencana dan meminimalkan dampaknya.
Baik	Organisasi ini memiliki rencana pemulihan bencana yang sangat baik dan teruji. Rencana ini mencakup langkah-langkah yang rinci dan jelas untuk mengatasi berbagai jenis bencana dan gangguan layanan.

Tabel 4.1.10 Umpan Balik Manajemen Keamanan Operasional

Nilai	Umpan Balik
Tidak Layak	Kontrol ini tidak memenuhi kerangka dasar yang diperlukan untuk memastikan operasi keamanan yang efektif. Pemantauan, pemeliharaan, dan perlindungan sistem tidak dilaksanakan dengan cukup, meninggalkan celah dalam keamanan dan berisiko untuk menghadapi ancaman keamanan.
Memenuhi Kerangka Dasar	Kontrol ini memenuhi kerangka dasar untuk memastikan operasi keamanan yang efektif melalui pemantauan, pemeliharaan, dan perlindungan sistem. Namun, masih ada beberapa aspek yang perlu diperbaiki untuk mencapai tingkat keamanan yang optimal.
Cukup Baik	Kontrol ini cukup baik dalam memastikan operasi keamanan yang efektif melalui pemantauan, pemeliharaan, dan perlindungan

	sistem. Sebagian besar kebutuhan keamanan terpenuhi, tetapi ada beberapa ruang untuk peningkatan dan penyesuaian untuk menghadapi perkembangan ancaman keamanan yang lebih baru.
Baik	Kontrol telah diimplementasikan dengan baik dan mencakup aspek-aspek penting yang diperlukan untuk melindungi sistem dari ancaman keamanan. Dengan adanya kontrol ini, risiko keamanan dapat dikelola dengan baik dan sistem dapat beroperasi dalam kondisi yang lebih aman.

Tabel 4.1.11 Umpan Balik Keamanan Komunikasi dan Operasi

Nilai	Umpan Balik
Tidak Layak	Kontrol ini tidak terlaksana dengan baik, mengakibatkan potensi kerentanannya dalam perlindungan informasi saat diproses, disimpan, dan ditransmisikan. Kelemahan dalam implementasi kontrol ini dapat menyebabkan pelanggaran keamanan dan risiko serius terhadap informasi sensitif.
Memenuhi Kerangka Dasar	Kontrol ini telah dipenuhi secara dasar dengan beberapa upaya untuk melindungi informasi saat diproses, disimpan, dan ditransmisikan. Namun, masih ada ruang untuk peningkatan dalam implementasi, pemantauan, dan pemeliharaan kontrol untuk mencapai tingkat keamanan yang lebih tinggi.
Cukup Baik	Kontrol ini telah diimplementasikan secara memadai dengan tindakan yang efektif dalam melindungi informasi saat diproses, disimpan, dan ditransmisikan. Upaya yang cukup baik telah dilakukan untuk mengurangi risiko keamanan, namun ada beberapa aspek yang dapat diperbaiki untuk memastikan keamanan yang lebih kuat.
Baik	Kontrol ini telah diimplementasikan dengan sangat baik dan efisien. Informasi saat diproses, disimpan, dan ditransmisikan dilindungi secara efektif dengan tindakan pencegahan dan pengamanan yang tepat. Organisasi telah mencapai tingkat keamanan yang sesuai dengan standar industri dan dapat diandalkan dalam melindungi informasi sensitif.

Tabel 4.1.12 Umpan Balik Pengendalian Akses Sistem Informasi

Nilai	Umpan Balik

Tidak Layak	Kontrol keamanan ini tidak diimplementasikan atau hanya terdapat upaya yang minim dalam mencegah akses yang tidak sah atau tidak pantas ke sistem informasi. Kebijakan dan mekanisme pengendalian akses belum disusun atau belum dijalankan dengan baik, meninggalkan celah bagi potensi ancaman keamanan yang dapat mengakibatkan akses yang tidak sah ke informasi kritis.
Memenuhi Kerangka Dasar	Kontrol keamanan ini sebagian besar telah diimplementasikan dengan mengacu pada kerangka dasar kebijakan dan mekanisme pengendalian akses. Namun, beberapa area mungkin masih perlu perbaikan atau pembaruan untuk menutup celah keamanan yang mungkin ada.
Cukup Baik	Kontrol keamanan ini secara substansial telah diterapkan dan sesuai dengan kebijakan dan mekanisme pengendalian akses.Pihak yang berwenang secara aktif mengawasi dan melacak aktivitas akses, dan tindakan pencegahan lanjutan dilakukan secara proaktif untuk mengatasi potensi masalah keamanan.
Baik	Kontrol keamanan ini telah diimplementasikan secara menyeluruh, efektif, dan efisien.

Tabel 4.1.13 Umpan Balik Perolehan, Pengembangan, dan Pemeliharaan Sistem Informasi

Nilai	Umpan Balik
Tidak Layak	Kontrol keamanan ini tidak diterapkan sepenuhnya dalam siklus hidup pengembangan sistem informasi, menyebabkan risiko potensial terhadap keamanan informasi dan kemungkinan terjadinya celah keamanan. Organisasi perlu segera memperhatikan dan mengatasi kekurangan dalam mengintegrasikan aspek keamanan dalam seluruh tahapan pengembangan sistem informasi.
Memenuhi Kerangka Dasar	Organisasi telah menciptakan kerangka dasar untuk mengintegrasikan keamanan dalam siklus hidup pengembangan sistem informasi. Namun, penerapan dan kepatuhan terhadap kontrol ini mungkin belum konsisten di seluruh proses pengembangan. Perlu dilakukan evaluasi lebih lanjut dan perbaikan untuk memastikan penerapan yang konsisten dan efektif.
Cukup Baik	Organisasi telah berhasil mengintegrasikan aspek keamanan dalam sebagian besar tahapan pengembangan, namun beberapa bagian

	mungkin masih terlalu lemah atau kurang terdefinisi dengan baik.
Baik	Organisasi telah berhasil mengintegrasikan keamanan secara holistik dalam seluruh siklus hidup pengembangan sistem informasi.

Tabel 4.1.14 Umpan Balik Pengelolaan Ketidaksesuaian

Nilai	Umpan Balik
Tidak Layak	Organisasi tidak memiliki prosedur yang tepat untuk menangani insiden keamanan, sehingga dapat menyebabkan eskalasi masalah dan meningkatkan risiko keamanan keseluruhan. Selain itu, juga tidak ada rencana tindakan yang jelas untuk mengurangi dampak dari insiden keamanan yang terjadi.
Memenuhi Kerangka Dasar	Organisasi memiliki beberapa prosedur dan kebijakan yang relevan untuk mengidentifikasi, mengelola, dan menangani insiden keamanan dan pelanggaran keamanan yang terjadi. Namun, beberapa aspek mungkin belum sepenuhnya tertutupi atau terdokumentasi dengan jelas. Reaksi terhadap insiden keamanan mungkin terkadang kurang terkoordinasi, dan analisis akar penyebab pelanggaran keamanan mungkin perlu ditingkatkan.
Cukup Baik	Organisasi secara aktif menerapkan kebijakan dan prosedur yang efektif untuk mengidentifikasi, mengelola, dan menangani insiden keamanan serta pelanggaran keamanan yang terjadi. Tim keamanan sering melakukan analisis akar penyebab insiden untuk mengurangi kemungkinan terulangnya peristiwa serupa di masa depan. Namun, ada ruang untuk meningkatkan reaksi terhadap insiden keamanan yang lebih cepat dan lebih terkoordinasi serta untuk memperbaiki laporan dan dokumentasi insiden.
Baik	Organisasi telah berhasil menerapkan kontrol keamanan ini dengan sangat baik.

Tabel 4.1.15 Umpan Balik Aspek Keamanan Pada Hubungan Bisnis

Nilai	Umpan Balik
Tidak Layak	Organisasi tidak memiliki kebijakan formal atau prosedur yang mengatur perlindungan informasi saat menjalin hubungan bisnis dengan pihak eksternal. Ini dapat menyebabkan kebocoran data,

	risiko pencurian informasi, atau ketidakmampuan untuk mengidentifikasi ancaman keamanan yang mungkin timbul dari keterlibatan pihak eksternal.
Memenuhi Kerangka Dasar	Organisasi telah mengadopsi kebijakan formal yang mengatur dan melindungi informasi selama berhubungan bisnis dengan pihak eksternal. Selain itu, kebijakan ini harus mencakup penilaian risiko, kontrak kerahasiaan, dan pembatasan akses informasi yang tepat. Meskipun demikian, implementasi dan pemantauan dapat ditingkatkan untuk memastikan keamanan informasi yang lebih kuat.
Cukup Baik	Organisasi memiliki kebijakan yang jelas dan komprehensif yang melindungi informasi selama berhubungan bisnis dengan pihak eksternal. Selain itu, kebijakan ini telah diimplementasikan secara efektif dan diikuti oleh seluruh anggota organisasi. Pemantauan dan penilaian risiko secara berkala juga dilakukan untuk memastikan kebijakan tetap relevan dan efektif menghadapi ancaman keamanan yang terus berkembang.
Baik	Organisasi memiliki kebijakan yang kuat, sistematis, dan dijalankan secara konsisten untuk melindungi informasi selama menjalin hubungan bisnis dengan pihak eksternal.

Tabel 4.1.16 Umpan Balik Kepatuhan Terhadap Standar

Nilai	Umpan Balik
Tidak Layak	Organisasi belum memiliki prosedur formal untuk mengidentifikasi dan memastikan kepatuhan dengan persyaratan hukum, regulasi, dan standar industri yang berlaku. Kebijakan yang ada tidak mencakup panduan khusus mengenai pemenuhan persyaratan hukum terkini.
Memenuhi Kerangka Dasar	Organisasi memiliki kerangka dasar untuk memastikan kepatuhan dengan persyaratan hukum, regulasi, dan standar industri. Namun, belum ada langkah-langkah rinci yang ditetapkan untuk menerapkan persyaratan ini ke dalam operasi sehari-hari. Beberapa dokumen kebijakan telah disusun, tetapi belum ada proses yang jelas untuk mengidentifikasi dan meninjau perubahan hukum atau regulasi yang relevan secara teratur.
Cukup Baik	Organisasi telah menetapkan kebijakan dan prosedur formal untuk memastikan kepatuhan dengan persyaratan hukum, regulasi, dan standar industri yang berlaku. Ada tim khusus atau personil yang

	ditugaskan untuk memantau perubahan hukum yang relevan dan memastikan kebijakan internal selaras dengan perubahan tersebut. Namun, belum ada langkah-langkah konkret yang dilakukan untuk mengukur efektivitas kepatuhan secara reguler atau mengevaluasi risiko kepatuhan.
Baik	Organisasi telah mengadopsi pendekatan sistematis untuk memastikan kepatuhan dengan persyaratan hukum, regulasi, dan standar industri yang berlaku.

Tabel 4.1.17 Umpan Balik Audit Keamanan Informasi

Nilai	Umpan Balik
Tidak Layak	Organisasi tidak memiliki proses audit keamanan informasi yang terstruktur dan terjadwal. Tidak ada upaya yang jelas untuk mengevaluasi secara teratur efektivitas kontrol keamanan informasi. Karena tidak ada audit yang dilakukan, potensi risiko dan kerentanannya tidak teridentifikasi secara sistematis, meninggalkan organisasi rentan terhadap ancaman keamanan yang tidak terdeteksi.
Memenuhi Kerangka Dasar	Organisasi telah menetapkan proses audit keamanan informasi yang dasar dan terjadwal. Audit dilakukan sesuai dengan jadwal tertentu, tetapi mungkin tidak selalu komprehensif atau mendalam. Meskipun telah ada upaya untuk memenuhi kerangka dasar ISO 27002, proses audit masih membutuhkan peningkatan agar menjadi lebih komprehensif dan efektif.
Cukup Baik	Organisasi secara teratur melakukan audit keamanan informasi sesuai dengan kerangka dasar ISO 27002. Proses audit terjadwal dan mencakup sebagian besar kontrol keamanan informasi yang relevan. Hasil audit dijadikan dasar untuk melakukan perbaikan dan peningkatan pada kontrol keamanan yang tidak memenuhi standar yang ditetapkan. Meskipun audit telah dilakukan dengan baik, masih ada ruang untuk meningkatkan ketelitian dan mendalamnya evaluasi agar menghadapi ancaman keamanan yang semakin kompleks.
Baik	Organisasi secara konsisten dan teratur melakukan audit keamanan informasi sesuai dengan standar ISO 27002.

Tabel 4.1.18 Bobot Jawaban Assessment

Jawaban	Bobot
Tidak dilakukan	0
Dalam perencanaan	1
Diterapkan sebagian	2
Diterapkan Menyeluruh	3

Pada Tabel 4.1.17, merupakan bobot jawaban dari setiap assessment kontrol keamanan ISO 27002, nilai paling tinggi adalah 3 yaitu kontrol keamanan telah diterapkan menyeluruh, lalu hasil dari assessment akan dikalkulasikan dan dianalisa berdasarkan standar rentang nilai ISO 27002 di Tabel 4.1.2 Rentang Nilai ISO 27002.

4.1.5.Pemodelan Sistem

Pemodelan sistem dalam penelitian Aplikasi Assessment dilakukan untuk menganalisis dan meningkatkan keamanan sistem informasi internal pada sebuah oragnisasi. Penelitian ini mengidentifikasi ruang lingkup sistem informasi dan aktivitas yang terlibat, menggunakan diagram aliran data dan proses. Dengan mengacu pada standar ISO 27002, peneliti mengevaluasi kepatuhan sistem terhadap praktik keamanan yang direkomendasikan. Ancaman dan kerentanan sistem juga diidentifikasi. Hasilnya berupa rekomendasi perbaikan, seperti meningkatkan teknologi keamanan, memperbarui kebijakan, dan memberikan pelatihan keamanan kepada staf. Tujuannya adalah untuk memastikan sistem informasi lebih aman dan terlindungi dari ancaman keamanan.

4.1.6.Prototype

Aplikasi yang dikembangkan dalam penelitian ini bertujuan untuk melakukan evaluasi keamanan sistem informasi berdasarkan standar ISO 27002.

Adapun fitur yang dikembangkan dalam penelitian ini sebagai berikut:

a. Login dan Manajemen Pengguna: Aplikasi ini menyediakan sistem autentikasi yang aman untuk pengguna yang diizinkan.
b. Penilaian Keamanan: Pengguna dapat mengisi kuesioner yang dirancang berdasarkan standar ISO 27002. Kuesioner ini mencakup berbagai aspek keamanan sistem informasi seperti kebijakan, pengendalian akses, keamanan fisik, manajemen risiko, dan sebagainya.
c. Evaluasi Risiko: Aplikasi ini menggunakan kuesioner yang diisi oleh pengguna untuk melakukan analisis risiko sistem informasi. Dengan mengidentifikasi kerentanannya, sistem memberikan peringkat risiko dan menampilkan area yang memerlukan perbaikan segera.
d. Rekomendasi Perbaikan: Berdasarkan hasil evaluasi risiko, aplikasi akan menghasilkan rekomendasi untuk perbaikan dan penerapan kebijakan yang sesuai dengan standar ISO 27002. Rekomendasi ini disajikan dalam bentuk langkah-langkah konkret untuk memperkuat keamanan sistem.
e. Riwayat Evaluasi: Aplikasi ini menyimpan riwayat penilaian keamanan sebelumnya, sehingga pengguna dapat melacak perubahan dan perkembangan sistem informasi dari waktu ke waktu.

4.2.Analisis dan Rancangan Sistem

Berikut adalah pendekatan metodologi yang digunakan untuk memahami, merencanakan, dan mengembangkan aplikasi *risk assessment*.

4.2.1.Analisis

Berikut adalah langkah-langkah analisis yang dilakukan dalam penelitian:

a. Studi ISO 27002: Melakukan studi mendalam terhadap standar ISO 27002 yang berkaitan dengan keamanan sistem informasi. Memahami setiap kriteria, kontrol, dan praktik yang dijelaskan dalam dokumentasi.
b. Identifikasi Risiko: Mengidentifikasi berbagai ancaman keamanan yang mungkin terjadi dalam sistem informasi. Melakukan analisis terhadap aspek-aspek keamanan seperti kehilangan data, serangan malware, serangan fisik, dan lain-lain.
c. Pembuatan Basis Pengetahuan: Membangun basis pengetahuan yang berisi aturan-aturan berdasarkan ISO 27002. Aturan-aturan ini akan digunakan oleh aplikasi *risk assessment* untuk melakukan penilaian risiko. Basis pengetahuan juga mencakup skala penilaian risiko berdasarkan standar ISO 27002.
d. Implementasi Aplikasi: Menerapkan teknik pemrograman dan menggunakan platform Node.js atau bahasa pemrograman JavaScript untuk mengimplementasikan aplikasi *risk assessment*. Aplikasi *risk assessment* ini akan menggabungkan pengetahuan dari basis pengetahuan dengan standar ISO 27002 untuk melakukan penilaian risiko.
e. Pengujian dan Evaluasi: Melakukan pengujian terhadap aplikasi *risk assessment* untuk memastikan keakuratannya dalam menilai risiko keamanan sistem informasi. Evaluasi juga dilakukan untuk mengukur efektivitas aplikasi *risk assessment* dalam memberikan rekomendasi tindakan yang sesuai.

4.2.2.Rancangan Sistem

Berikut adalah komponen-komponen dalam aplikasi untuk Risk Assessment Keamanan Sistem Informasi berdasarkan ISO 27002:

a. Antarmuka Pengguna: Terdapat antarmuka pengguna yang memungkinkan pengguna memasukkan informasi terkait sistem informasi yang akan dinilai risikonya. Pengguna akan mengisi *assessment* tentang sistem informasi, kontrol keamanan yang ada, dan potensi ancaman yang dapat muncul. Antarmuka aplikasi *risk assessment* ini dibangun menggunakan library React.js.
b. Modul Penilaian Risiko: Modul ini akan menggunakan basis pengetahuan yang telah dibangun berdasarkan ISO 27002 untuk melakukan penilaian risiko. Nilai ISO 27002 akan digunakan untuk menghitung tingkat kepercayaan terhadap risiko yang ada.
c. Modul Rekomendasi: Setelah penilaian risiko dilakukan, modul ini akan memberikan rekomendasi tindakan yang harus diambil berdasarkan tingkat risiko yang ditentukan. Rekomendasi dapat berupa tindakan pencegahan, perbaikan kontrol keamanan, atau langkah-langkah lain yang sesuai.
d. Basis Pengetahuan: Basis pengetahuan akan berisi aturan-aturan yang merujuk pada standar ISO 27002 dan pengetahuan domain yang relevan. Basis pengetahuan ini akan diakses oleh modul penilaian risiko dan modul rekomendasi.
e. Data Pengetahuan: Data Pengetahuan ini akan menyimpan data terkait dengan sistem informasi yang dinilai risikonya, kontrol keamanan yang diterapkan,

ancaman yang diidentifikasi, serta riwayat penilaian risiko dan rekomendasi tindakan sebelumnya kedalam basis data *firestore.*

f. Logika Penalaran: Logika penalaran akan digunakan oleh aplikasi untuk melakukan inferensi berdasarkan aturan-aturan yang ada dalam basis pengetahuan. Penalaran memungkinkan aplikasi untuk mengambil keputusan yang tepat berdasarkan informasi yang diberikan oleh pengguna.
g. Sistem Manajemen: Sistem ini akan bertanggung jawab untuk mengelola data dan menjaga keberlanjutan operasional aplikasi *risk assessment*. Hal ini meliputi pemeliharaan basis pengetahuan, manajemen akses pengguna, serta pencatatan riwayat penilaian risiko dan rekomendasi.

4.3.Implementasi

Berikut adalah proses implementasi Aplikasi untuk Risk Assessment Keamanan Sistem Informasi Berdasarkan ISO 27002.

4.3.1.Pemilihan Teknologi

Teknologi yang digunakan dalam pembuatan aplikasi *risk assessment* adalah Next.js dan basis data Firestore, Next.js adalah sebuah kerangka kerja (framework) React yang digunakan untuk membangun aplikasi web berbasis server-side rendering (SSR) dan static site generation (SSG). Pemilihan teknologi ini memiliki beberapa alasan:

f. Server-side Rendering (SSR) dan Static Site Generation (SSG): Karena ini adalah aplikasi *risk assessment* yang mungkin akan digunakan oleh banyak pengguna, SSR dan SSG membantu memastikan bahwa konten halaman akan di-render dan diambil dari sisi server sebelum dikirim ke klien, mengurangi beban server dan meningkatkan performa.

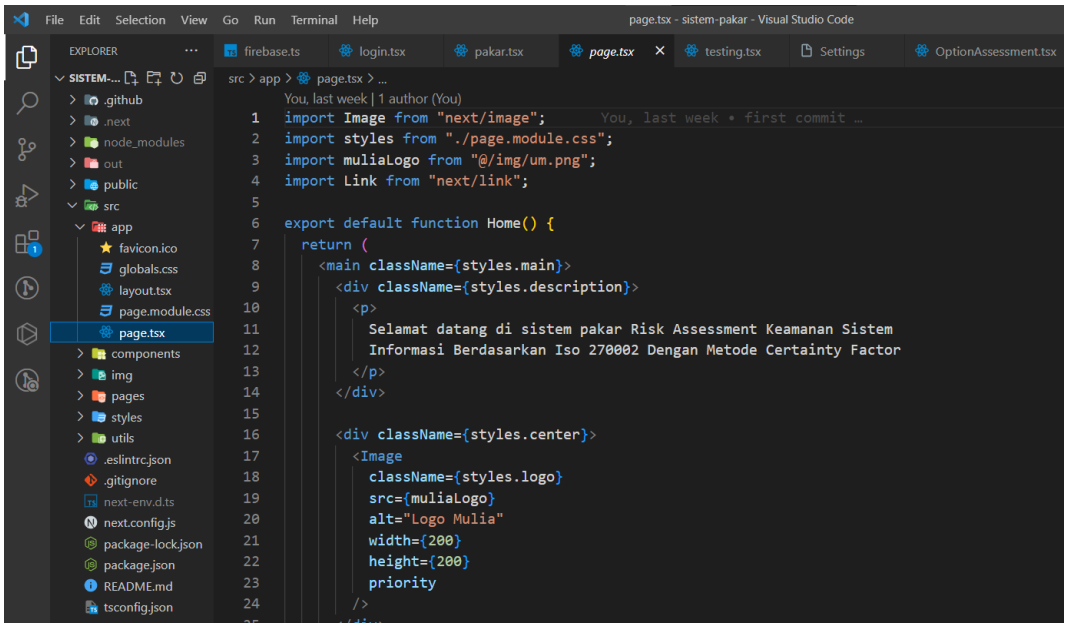
g. SEO Friendly: Next.js memungkinkan konten aplikasi di-render pada sisi server sebelum dikirimkan ke klien, yang dapat meningkatkan kemampuan SEO dan membantu aplikasi mudah ditemukan oleh mesin pencari.

h. Pengembangan React yang Efisien: Next.js berbasis pada React, yang merupakan salah satu pustaka JavaScript populer untuk membangun antarmuka pengguna yang responsif dan interaktif.

i. Dukungan Komunitas dan Pertumbuhan Ekosistem: Next.js telah menjadi kerangka kerja yang populer dalam komunitas pengembang web. Dengan begitu banyaknya sumber daya, dokumentasi, dan dukungan dari komunitas, penelitian ini dapat memanfaatkan ekosistem yang berkembang pesat.

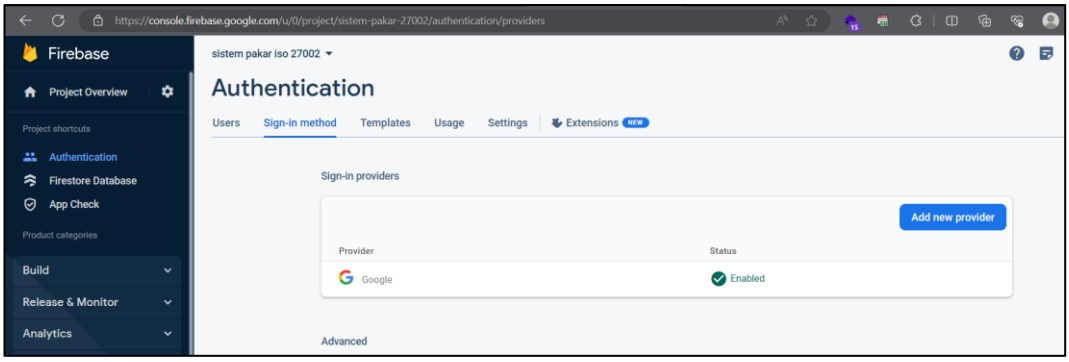
4.3.2.Pengembangan Backend

Pengembangan backend dimulai dengan inisialisasi project, yaitu menyiapkan struktur dan konfigurasi awal yang diperlukan dalam proses pengembangan selanjutnya.



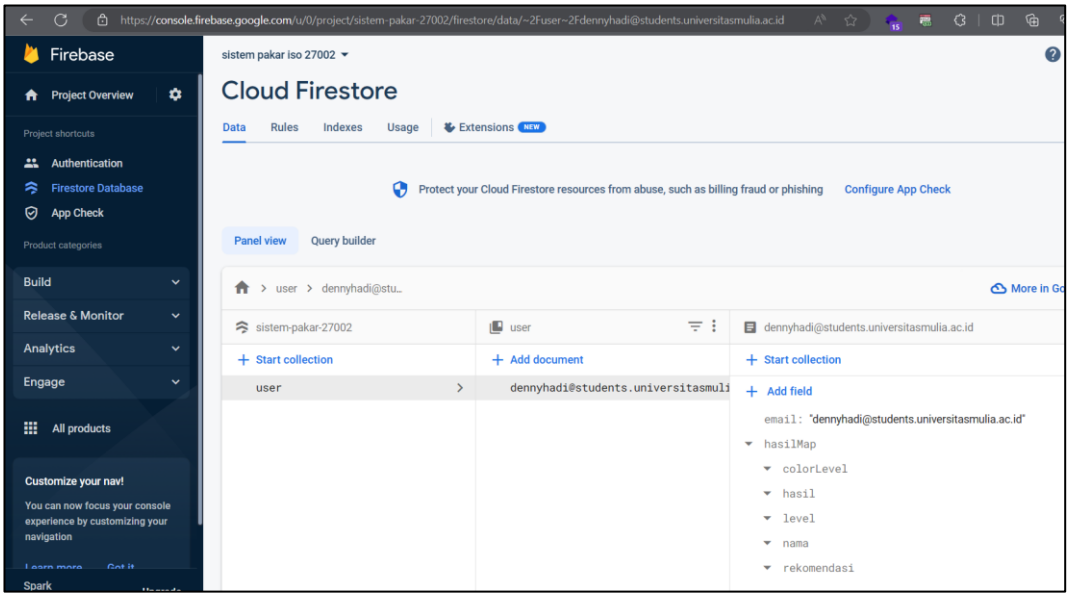
Gambar 4.3.1 Inisialisasi Project

Setelah inisialisasi project, selanjutnya mengkonfigurasi Firebase Authentication, yaitu sebuah layanan otentikasi pengguna yang disediakan oleh Firebase. Firebase Authentication memungkinkan integrasi sistem otentikasi ke dalam aplikasi *risk assessment*.



Gambar 4.3.2 Konfigurasi Firebase Authentication

Pada Gambar 4.3.2, konfigurasi Firebase authentication hanya mengizinkan otentikasi melalui akun Google. Setelah selesai konfigurasi otentikasi, selanjutnya membuat struktur basis data menggunakan layanan basis data Firestore, agar data assessment pengguna dapat diakses kembali secara fleksibel dan skala besar dalam aplikasi aplikasi *risk assessment*.



Gambar 4.3.3 Struktur Basis Data Firestore

Pada skema basis data yang dibuat di Gambar 4.3.3, koleksi di definisikan dengan nama user, di dalam koleksi user, berisi daftar dokumen yang di definisikan dengan email pengguna dan di setiap data pengguna berisi *string* email dan *mapping* hasilMap. *String* email digunakan untuk menyimpan email pengguna, sekaligus dijadikan kunci utama untuk mengakses data dan mapping hasilMap adalah data dengan tipa data *mapping* yang berisi *array* hasil assessment pengguna, yaitu colorLevel[], hasil[], level[], nama[] dan rekomendasi[].

4.3.3.Implementasi Basis Pengetahuan

Aplikasi *risk assessment* ini memiliki basis pengetahuan untuk pemahaman, formulasi, dan juga skema penyelesaian masalah. Basis pengetahuan yang digunakan dalam aplikasi ini yaitu dokumentasi ISO/IEC 27002:2013 yang merujuk pada assessment di **Tabel 4.1.1 14 Kontrol Keamanan ISO 27002** yang berisi 14 kontrol keamanan.

Rentang nilai dari keseluruhan assessment digunakan sebagai parameter kategori risiko, berdasarkan **Tabel 4.1.2 Rentang Nilai ISO 27002**, sebagai hasil akhir penilaian assessment risiko. Maka rumus yang digunakan sebagai berikut:

"Nilai assessment = total nilai risiko"
(ISO/IEC 27002:2013)

Gambar 4.3.4 Rumus Nilai Assessment

Setelah diketahui nilai assessment, selanjutnya aplikasi akan menampilkan nilai kategori risiko, berdasarkan nilai ISO 27002 pada **Tabel 4.1.2 Rentang Nilai ISO 27002.**

```
// total skor
switch (true) {
  case total == 0 || total <= 50:
    level = "Risiko Tinggi";
    colorLevel = "error";
    rekomendasi = `===Hasil Analisa===\n\nRisiko
    break;
  case total == 51 || total <= 99:
    level = "Risiko Sedang";
    colorLevel = "warning";
    rekomendasi = `===Hasil Analisa===\n\nRisiko
    break;
  case total == 100 || total <= 199:
    level = "Risiko Rendah";
    colorLevel = "primary";
    rekomendasi = `===Hasil Analisa===\n\nRisiko
    break;
  case total == 200 || total <= 294:
    level = "Risiko Sangat Rendah";
    colorLevel = "success";
    rekomendasi = `===Hasil Analisa===\n\nRisiko
    break;
  default:      You, last week • custom color lev
    level = "Risiko Tinggi";
    colorLevel = "error";
    rekomendasi = `===Hasil Analisa===\n\nRisiko
    break;
}
```

Gambar 4.3.5 Implementasi Nilai Risiko

Pada Gambar 4.3.5, merupakan kode switch statement yang digunakan untuk menentukan **level risiko** berdasarkan nilai dari variabel **total**. Selain itu, kode ini juga mengatur pesan umpan balik (rekomendasi) dan warna (colorLevel) yang akan ditampilkan tergantung dari **nilai total** yang didapatkan dari hasil assessment.

Untuk mengimplementasikan *feedback* atau umpan balik dari setiap kontrol keamanan, digunakan penilaian berdasarkan **Tabel 4.1.3 Rentang Nilai Aspek Tiap Kontrol**. Maka rumus yang digunakan sebagai berikut:

“Nilai kontrol keamanan = total nilai assessment tiap kontrol”

(ISO/IEC 27002:2013)

Gambar 4.3.6 Rumus Nilai Kontrol Keamanan

Total nilai assessment diambil dari assessment yang diisi pengguna di setiap kontrol keamanan, tiap pilihan assessment memiliki bobot nilai berdasarkan **Tabel 4.1.18 Bobot Jawaban Assessment**.

Setelah didapatkan nilai kontrol keamanan, selanjutnya aplikasi akan menampilkan feedback sesuai data umpan balik pada **Tabel 4.1.4** sampai Tabel **4.1.17.**

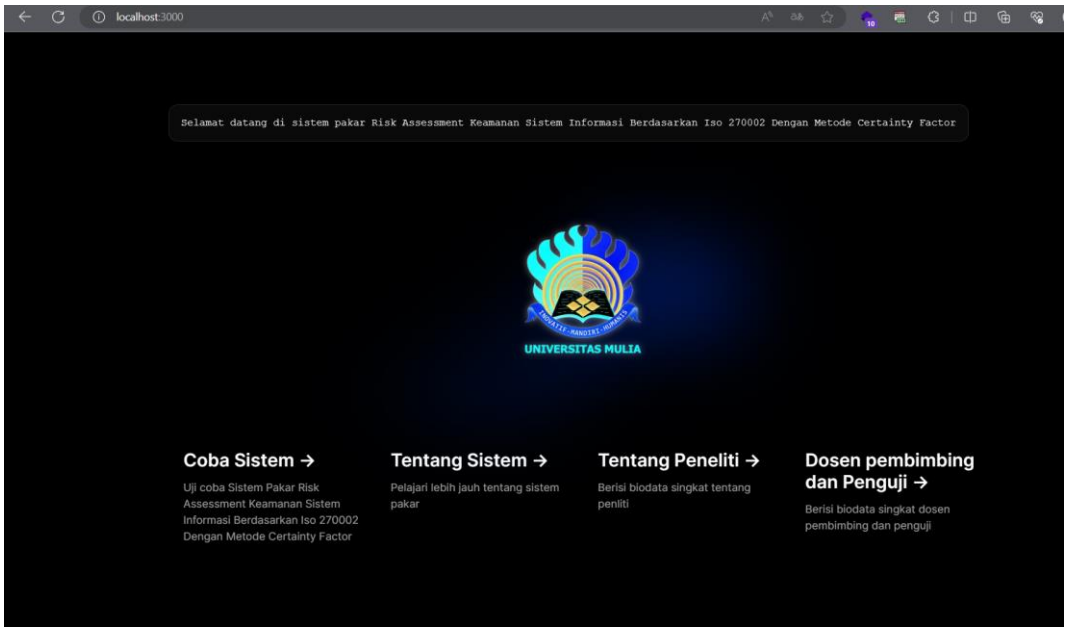
```
289     // kontrol 1
290     switch (true) {
291       case kontrol1 == 0:
292         resultKontrol1 =
293           "### Umpan balik Kebijakan keamanan informasi (Tidak Layak)\n\n Kontrol keamanan informasi ini
294         break;
295       case kontrol1 == 1 || kontrol1 <= 7:
296         resultKontrol1 =
297           "### Umpan balik Kebijakan keamanan informasi(Memenuhi Kerangka Dasar)\n\n Kontrol ini memenuhi
298         break;
299       case kontrol1 == 8 || kontrol1 <= 15:
300         resultKontrol1 =
301           "### Umpan balik Kebijakan keamanan informasi(Cukup Baik)\n\n Kontrol keamanan informasi ini cu
302         break;
303       case kontrol1 == 16 || kontrol1 <= 21:
304         resultKontrol1 =
305           "### Umpan balik Kebijakan keamanan informasi(Baik)\n\n Kontrol keamanan informasi ini sepenuhn
306         break;
307       default:
308         resultKontrol1 = "null";
309         break;
310     }
```

Gambar 4.3.7 Implementasi Nilai Kontrol Keamanan

Pada Gambar 4.3.7, merupakan sebuah switch statement yang digunakan untuk memberikan umpan balik (feedback) terhadap nilai dari variabel kontrol1 atau (Kebijakan keamanan informasi). Tujuan dari kode ini untuk menghasilkan pesan umpan balik yang berbeda tergantung pada nilai kontrol1 yang diberikan.

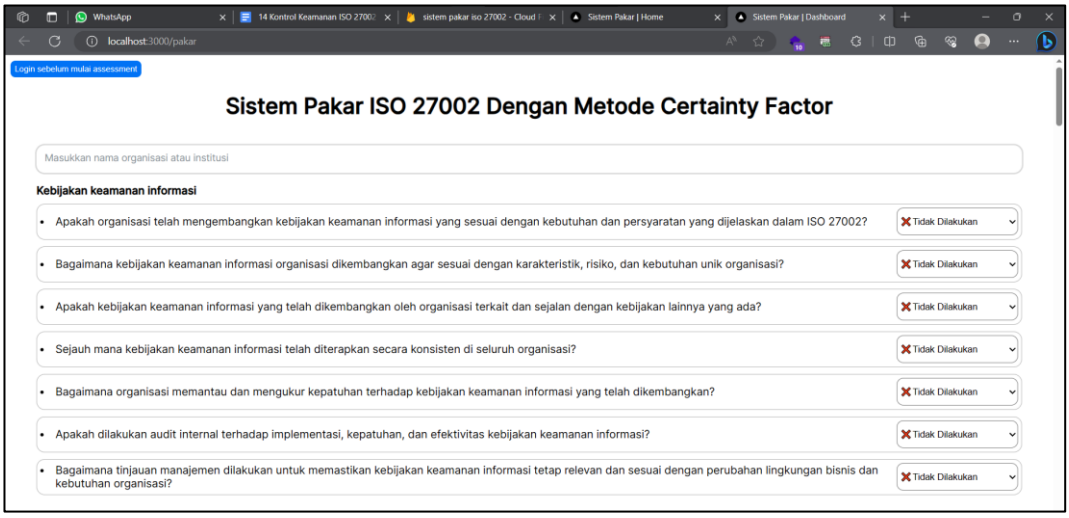
4.3.4.Pengembangan Frontend

Pengembangan frontend atau antarmuka pengguna aplikasi *risk assessment*, dibuat menggunakan pustaka React dan untuk mengatur tampilan atau gaya elemen dalam halaman web, peneliti menggunakan *css native* dan library Next.UI untuk komponen button serta input.



Gambar 4.3.8 Tampilan Home Aplikasi

Terlihat pada Gambar 4.3.4, merupakan tampilan home dari aplikasi *risk assessment* lengkap dengan logo Universitas Mulia yang menyatu dengan latar belakang.



Gambar 4.3.9 Tampilan Utama Aplikasi Risk Assessment

Pada Gambar 4.3.5, merupakan tampilan dashboard dari aplikasi *risk assessment*, disini pengguna dapat melakukan assessment terhadap keamanan sistem informasi.

4.4.Pengujian Sistem

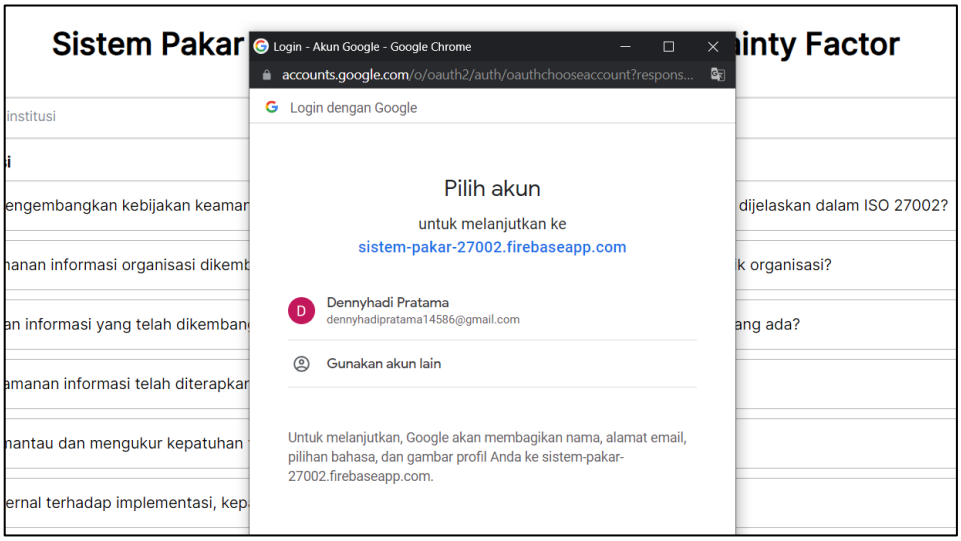
Pengujian sistem dalam penelitian ini terbagi menjadi dua, yaitu *white box testing* dan *black box testing*.

4.4.1.White Box Testing

Pengujian yang pertama yaitu *white box testing*, disini peneliti melakukan dua tahapan, *integration testing* dan *code coverage analysis*.

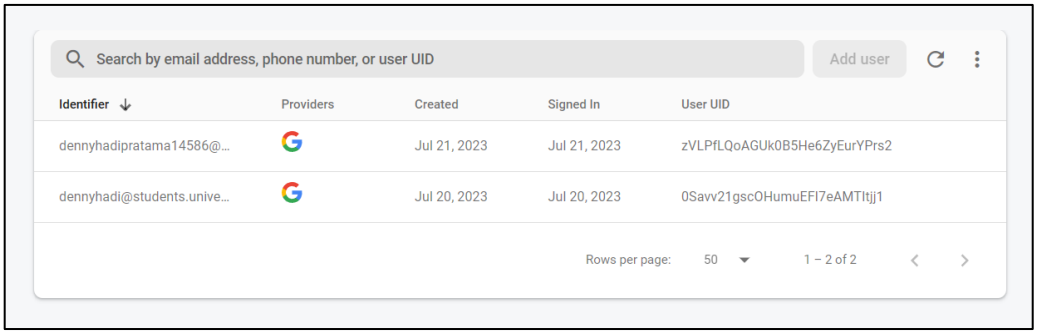
a. *Integration Testing*

Integration testing adalah tahapan menguji interaksi antara beberapa unit atau komponen untuk memastikan bahwa integrasinya berjalan dengan baik. Adapun integrasi yang diuji adalah otentikasi dan koneksi basis data.



Gambar 4.4.1 Testing Otentikasi

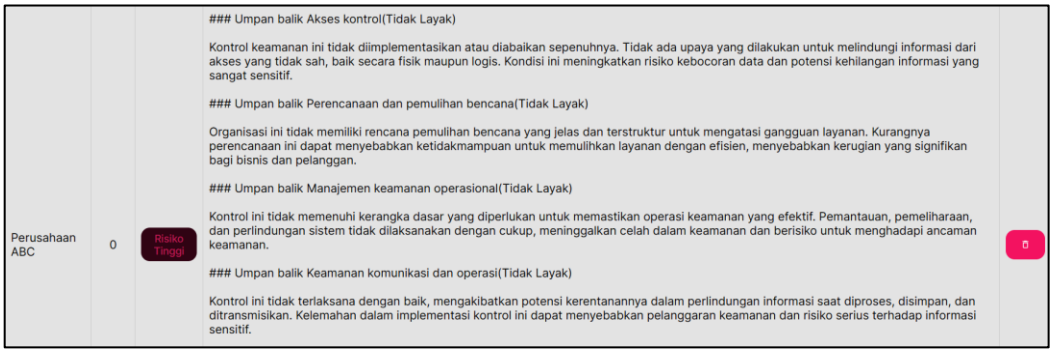
Pada Gambar 4.4.1, terlihat otentikasi berhasil dengan menggunakan akun Google. Setelah melakukan otentikasi, peneliti melakukan pengecekan data di basis data.



Gambar 4.4.2 Cek Akun di Basis Data

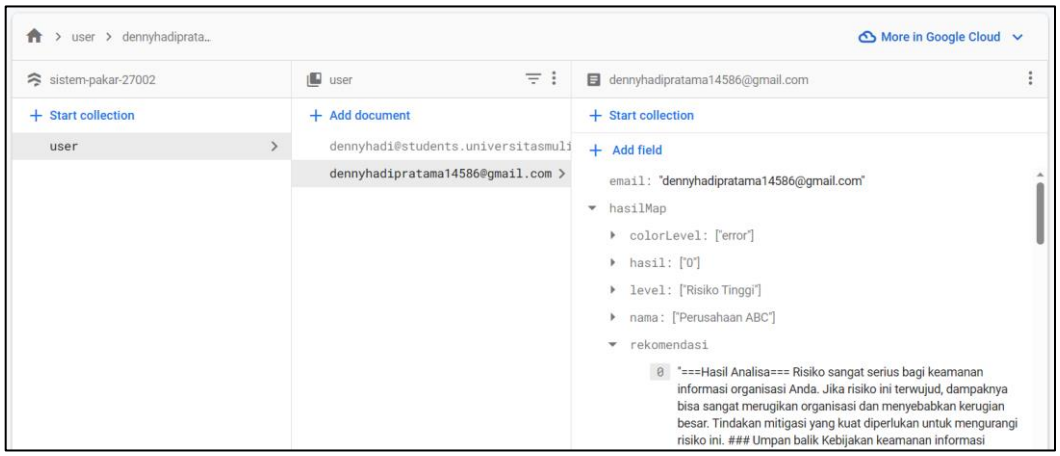
Pada Gambar 4.4.2, terlihat data pengguna terekam di basis data, hal ini menandakan otentikasi telah berhasil di integrasikan.

Setelah pengujian otentikasi selesai, peneliti selanjutnya menguji sistem aplikasi.



Gambar 4.4.3 Hasil Assessment Aplikasi Risk Assessment

Pada Gambar 4.4.3, aplikasi berhasil menghasilkan output berupa analisa dan umpan balik dari tiap domain atau kontrol keamanan ISO 27002. Selain itu, peneliti juga melakukan pengecekan di basis data, untuk memastikan data pengguna telah tersimpan.

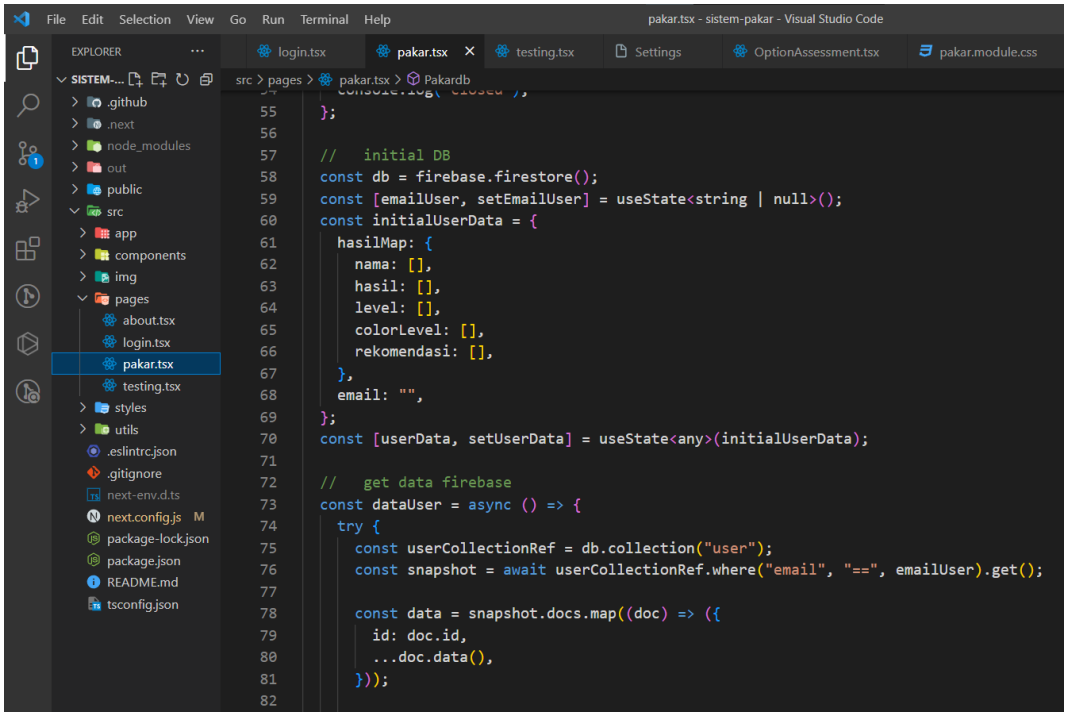


Gambar 4.4.4 Cek Assessment Pengguna

Pada Gambar 4.4.4, terlihat data assessment pengguna telah tersimpan di basis data dan dapat diakses kembali.

b. *Code Coverage Analysis*

Code coverage analysis yaitu proses melihat sejauh mana kode yang telah diuji dan dijalankan selama proses pengujian untuk memastikan semua kode tercakup.



Gambar 4.4.5 Kode Program Aplikasi Risk Assessment

Pada Gambar 4.4.5, terlihat tampilan dari kode program aplikasi *risk assessment* yang berisi komentar, struktur program dan juga penetapan tipe data secara statis untuk meminimalisir bug saat pengujian.

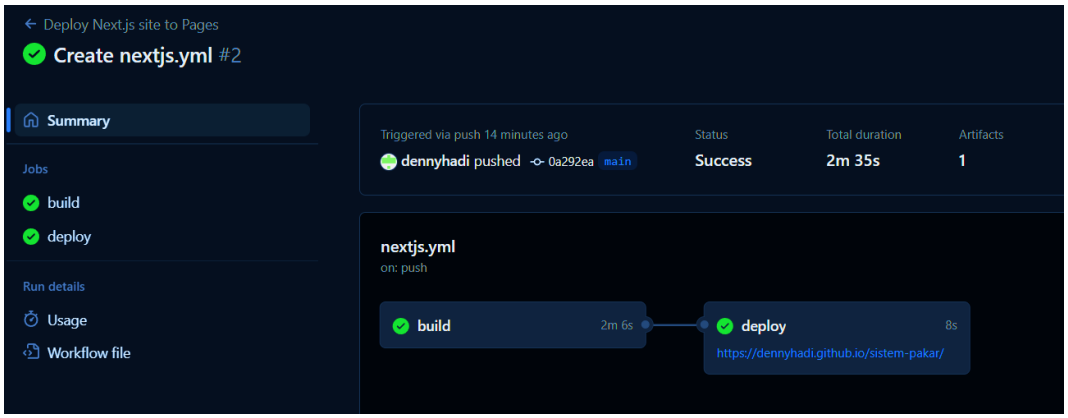
4.4.2.Black Box Testing

Pengujian *black box testing* yang dilakukan adalah validasi fitur sistem dan fungsionalitas perangkat lunak dari perspektif pengguna akhir. Adapun fitur yang telah divalidasi pengguna akhir meliputi integrasi otentikasi, *responsive design*, dan hasil *assessment* yang terekam di basis data. Dari semua fungsionalitas yang telah diuji, tidak ditemukan bug.

4.5.Peluncuran Sistem

Peluncuran sistem yang digunakan dalam penelitian adalah dengan memanfaatkan layanan *hosting* dari Github Pages, GitHub Pages memungkinkan

pengembang dengan cepat dan mudah menerbitkan situs web langsung dari repositori GitHub.

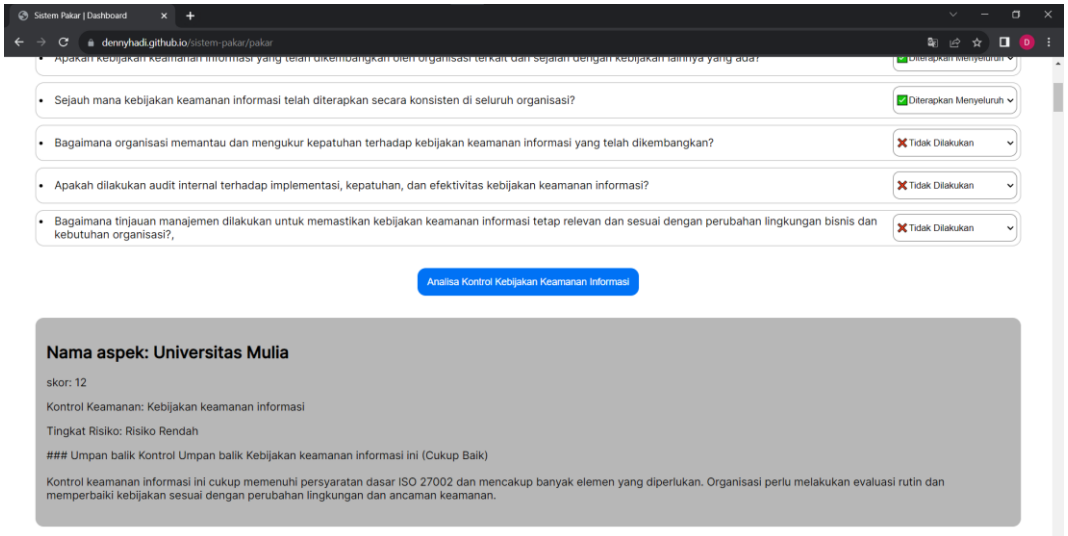


Gambar 4.5.1 Deploy Sistem

Pada Gambar 4.5.1, merupakan proses *build* dan *deploy* sebelum website dapat diakses secara online. Demo aplikasi secara publik dapat diakses di https://dennyhadi.github.io/sistem-pakar/pakar

4.6.Pengujian Aplikasi

Setelah selesai proses deploy sistem, selanjutnya menguji sistem pada sisi production, mulai dari login aplikasi sampai melakukan assessment.



Gambar 4.6.1 Pengujian Apliksai di Production

Pada Gambar 4.6.1, aplikasi berhasil berjalan lancar pada sisi production dan dapat memberikan umpan balik sesuai nilai ISO 27002.

BAB V

PENUTUP

5.1.Kesimpulan

Adapun kesimpulan penelitian sebagai berikut:

a. Dari hasil penelitian yang telah dilakukan, aplikasi risk assessment dapat memberikan umpan balik risiko dan keamanan sistem informasi yang bermanfaat berdasarkan, ISO 27002 sebagai pedoman utama yang relevan dan komprehensif.
b. Penggunaan standarisasi keamanan ISO 27002 dalam aplikasi *risk assessment* untuk penilaian risiko sistem informasi terbukti efektif. Metode ini memungkinkan integrasi tingkat keyakinan dari aturan-aturan yang digunakan dalam proses pengambilan keputusan, yang membantu meningkatkan akurasi dan kualitas penilaian risiko.
c. Aplikasi *risk assessment* yang dibangun dengan memadukan ISO 27002 dapat menjadi alat yang sangat berguna dalam membantu para profesional keamanan informasi dalam mengidentifikasi, mengevaluasi, dan mengelola risiko sistem informasi dengan lebih efisien dan akurat.

5.2.Saran

Adapun saran penelitian sebagai berikut:

a. Menambahkan lebih banyak sumber data terkait risiko keamanan sistem informasi akan meningkatkan akurasi dan ketepatan penilaian risiko.
b. Mempertimbangkan perluasan lingkup aplikasi *risk assessment* selain keamanan sistem informasi, aplikasi juga dapat dikembangkan untuk menilai

risiko keamanan pada aplikasi perangkat lunak, infrastruktur jaringan, dan sistem lainnya.

c. Melibatkan banyak profesional keamanan informasi dalam proses evaluasi dan pengujian aplikasi *risk assessment* akan memberikan wawasan dan umpan balik untuk meningkatkan kualitas serta relevansi aplikasi *risk assessment*.

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

ISO/IEC 27002:2013. Information technology — Security techniques — Code of practice for information security controls. Online pada https://www.iso.org/standard/54533.html diakses tanggal 21 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

Nidhra, S., & Dondeti, J. (2012). Black box and white box testing techniques-a literature review. *International Journal of Embedded Systems and Applications (IJESA)*, 2(2), 29-50. https://dx.doi.org/10.5121/ijesa.2012.2204

Taivalsaari, A., Mikkonen, T., Ingalls, D., & Palacz, K. (2008, September). Web browser as an application platform. In 2008 34th *Euromicro Conference Software Engineering and Advanced Applications* (pp. 293-302). IEEE. https://doi.org/10.1109/SEAA.2008.17

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

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

Petersen, K., Wohlin, C., & Baca, D. (2009). The waterfall model in large-scale development. In *Product-Focused Software Process Improvement: 10th International Conference, PROFES 2009, Oulu, Finland, June 15-17, 2009*. Proceedings 10 (pp. 386-400). Springer Berlin Heidelberg. https://dx.doi.org/10.1007/978-3-642-02152-7_29

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://ojs.stmik-banjarbaru.ac.id/index.php/jutisi/article/view/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://dx.doi.org/10.26438/ijcse/v5i12.301304

LAMPIRAN

Lampiran 1. ISO/IEC 27002:2013

Nederlandse norm

NEN-ISO/IEC 27002

(en)

Information technology - Security techniques -
Code of practice for information security controls
(ISO/IEC 27002:2013,IDT)

Vervangt NEN-ISO/IEC 27002:2007

ICS 35.040
oktober 2013