



**SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI**

**Asesmen Risiko Keamanan Informasi Sistem Informasi  
Penerimaan Mahasiswa pada STT-NF dengan SNI ISO/ IEC  
27001:2022**

**TUGAS AKHIR**

**Abdullah Mumtaz  
0110120002**

**Program Studi Sistem Informasi  
Depok  
Agustus 2024**



**SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI**

**Asesmen Risiko Keamanan Informasi Sistem Informasi  
Penerimaan Mahasiswa pada STT-NF dengan SNI ISO/ IEC  
27001:2022**

**TUGAS AKHIR**

**Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana**

**Abdullah Mumtaz**

**0110120002**

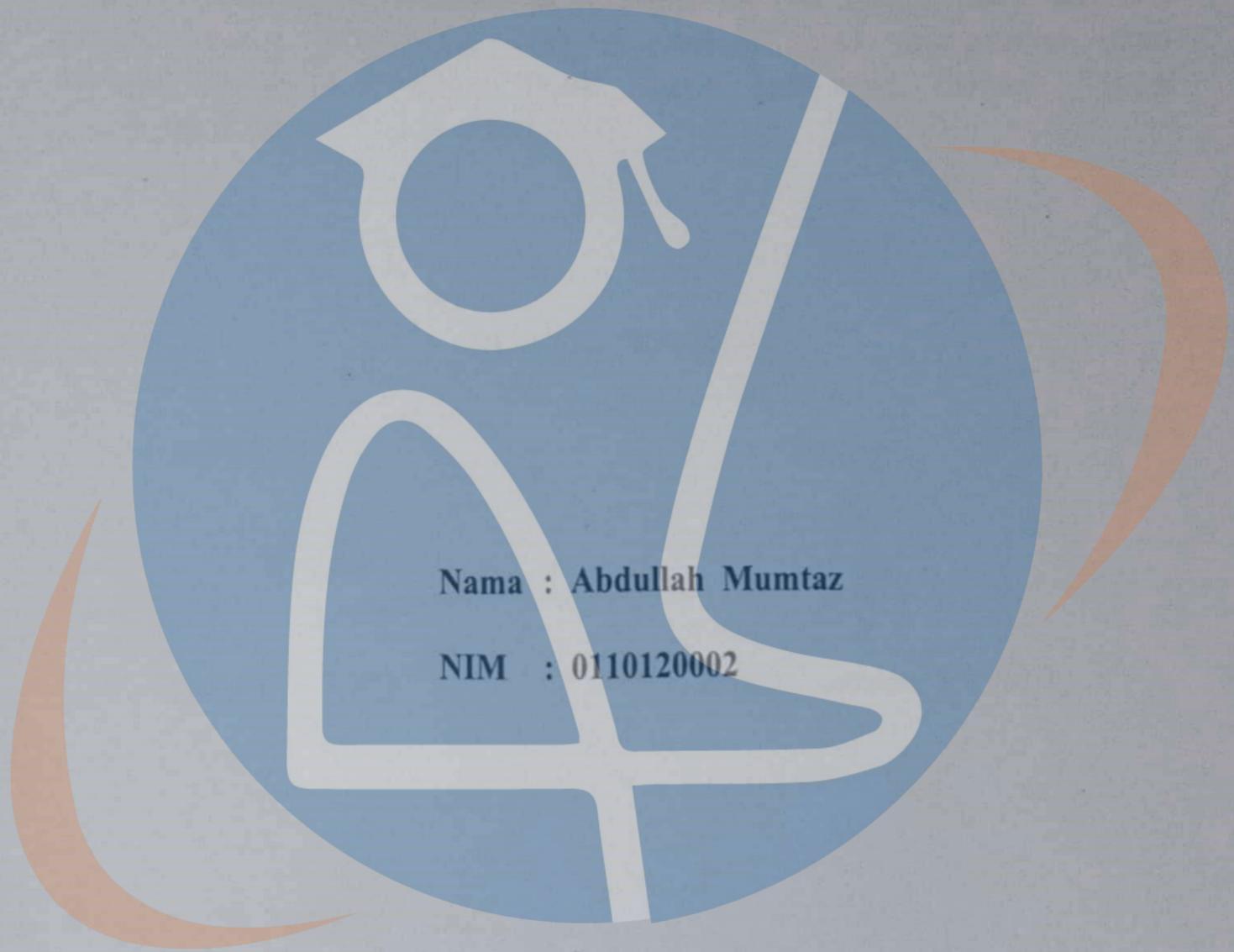
**STT - NF**  
**Program Studi Sistem Informasi**

**Depok**

**Agustus 2024**

## Halaman Pernyataan Orisinalitas

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



Nama : Abdullah Mumtaz

NIM : 0110120002

STT - NF

Depok, 5 Agustus 2024

Tanda Tangan

A handwritten signature in black ink, appearing to be 'Mumtaz'.

Abdullah Mumtaz

## Halaman Pengesahan

Skripsi/Tugas Akhir ini diajukan oleh:

Nama: Abdullah Mumtaz

NIM: 0110120002

Program Studi: Sistem Informasi

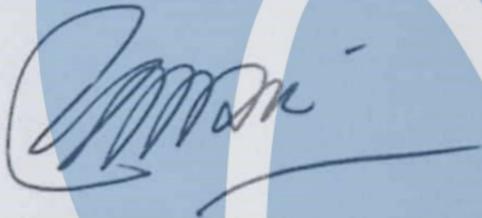
Judul Skripsi: Asesmen Risiko Keamanan Informasi Sistem Informasi

Penerimaan Mahasiswa pada STT-NF dengan SNI ISO/ IEC 27001:2022

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

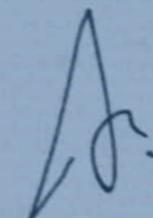
DEWAN PENGUJI

Pembimbing



(Drs. Rusmanto, M.M.)

Penguji



(Dr. Amalia Rahmah, S.T, M.T)

Ditetapkan di: Depok

Tanggal: 5 Agustus 2024

STT - NF

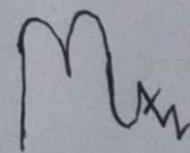
## Kata Pengantar

Penulis ingin mengucapkan terima kasih kepada Allah SWT atas kemampuan mereka untuk menyelesaikan tugas akhir ini berkat bantuan dan rahmat-Nya. Penulis menyadari bahwa akan sangat sulit menyelesaikan karya/skripsi ini tanpa bantuan dan bimbingan semua pihak mulai dari perkuliahan hingga penulisan karya ini.

1. Allah SWT.
2. Orang tua dan seluruh anggota keluarga yang telah memberikan dukungan moril dan materil dalam menjalankan tugas ini.
3. Bapak Dr. Lukman Rosyidi, S.T, M.M., M.T selaku Ketua Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
4. Ibu Misna Asqia, S.Kom, M.Kom Ketua Program Studi Sistem Informasi di Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
5. Ibu Dr. Amalia Rahmah, S.T, M.T. selaku Dosen Pembimbing Akademik yang telah membimbing penulis selama berkuliah di Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
6. Bapak Drs. Rusmanto, M.M. selaku Dosen Pembimbing Tugas Akhir penulis dalam menyelesaikan penulisan ilmiah ini.
7. Dosen di Sekolah Tinggi Teknologi Terpadu Nurul Fikri yang telah membantu penulis belajar.

Tentu saja dokumen akademis ini masih mempunyai banyak kekurangan karena keterbatasan pengetahuan dan kemampuan penulis. Namun, penulis berusaha menyelesaikan penelitian ini sepenuhnya. Oleh karena itu, penulis dengan senang hati menerima kritik dan saran dari pembaca jika karya akademik ini memiliki kekurangan.

Depok, 5 Agustus 2024



Abdullah Mumtaz

**Halaman Pernyataan Persetujuan  
Publikasi Tugas Akhir Untuk Kepentingan Akademis**

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

Nama: Abdullah Mumtaz

NIM: 0110120002

Program Studi: Sistem Informasi

Jenis karya: Skripsi / Tugas Akhir

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

**Asesmen Risiko Keamanan Informasi Sistem Informasi Penerimaan Mahasiswa pada STT-NF dengan SNI ISO/ IEC 27001:2022**

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

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di Depok

Pada tanggal: 5 Agustus 2024

Yang Menyatakan

  
(Abdullah Mumtaz)

## Abstrak

Nama : Abdullah Mumtaz  
NIM : 0110120002  
Program Studi : Sistem Informasi  
Judul : Asesmen Risiko Keamanan Informasi Sistem Informasi  
Penerimaan Mahasiswa pada STT-NF dengan SNI ISO/  
IEC 27001:2022

Dalam penelitian ini dilakukan asesmen risiko keamanan informasi untuk mengidentifikasi ancaman potensial terhadap aset yang terkait dengan pemrosesan data serta menentukan cara terbaik untuk melindungi aset tersebut. Tujuan penelitian ini adalah melaksanakan asesmen risiko pada Sistem Informasi Penerimaan Mahasiswa. Dampak negatif jika tidak ada asesmen risiko adalah kelemahan sistem tidak diketahui sehingga rentan terjadi peretasan karena tidak diketahui upaya-upaya yang harus dilakukan agar meminimalkan terjadi kasus peretasan. Tahapan yang dilalui yaitu melakukan wawancara untuk mendapatkan data setelah itu melakukan identifikasi aset lalu melakukan identifikasi risiko kemudian melakukan analisis risiko setelah analisis risiko terakhir dilanjutkan dengan evaluasi risiko. Analisis data yang diperlukan dilakukan melalui metode survei, yang merupakan bagian dari pendekatan penelitian kuantitatif. Analisis data kualitatif yang digunakan dalam penelitian ini adalah analisis data kualitatif deskriptif. Analisis data kualitatif ini menguraikan secara apa adanya. Analisis data kualitatif digunakan untuk mengolah data hasil pengujian dan evaluasi setelah penelitian ini selesai dilakukan. *Tools* yang digunakan dalam penelitian ini yaitu berbasis SNI ISO 27005:2022. Penerapan asesmen risiko untuk Sistem Informasi Penerimaan Mahasiswa dilakukan sesuai dengan panduan yang ada di dokumen SNI ISO 27005:2022. Proses asesmen risiko dimulai dari identifikasi risiko, analisis risiko, evaluasi risiko. Proses asesmen risiko sudah diuji dan berhasil. Dari hasil evaluasi menunjukkan perlu penelitian lebih lanjut yang mencakup keseluruhan aset informasi dan aset lain yang berkaitan dengan keamanan informasi pada Sistem Informasi Penerimaan Mahasiswa Baru STT-NF. Evaluasi menunjukkan penelitian lebih lanjut mencakup keseluruhan aset informasi dan aset lain berkaitan dengan keamanan informasi pada Sistem Informasi Penerimaan Mahasiswa Baru STT-NF, asesmen perlu dilakukan pada jenis klasifikasi aset.

Kata kunci: Asesmen risiko, SNI ISO 27005, SNI ISO 27001, risiko keamanan informasi, aset, keamanan, peretasan.

## Abstract

Name : Abdullah Mumtaz.

NIM : 0110120002

Study Program : Information System

Title : Information Security Risk Assessment of Student Admission Information System at STT-NF with SNI ISO / IEC 27001: 2022

*In this study, an information security risk assessment was conducted to identify potential threats to assets related to data processing and determine the best way to protect these assets. The purpose of this research is to carry out a risk assessment on the Student Admission Information System. The negative impact if there is no risk assessment is that the weaknesses of the system are unknown so that it is vulnerable to hacking because it is not known what efforts must be made to minimise hacking cases. The steps taken are conducting interviews to obtain data after that identifying assets then identifying risks then conducting risk analysis after the last risk analysis followed by risk evaluation. The necessary data analysis is carried out through the survey method, which is part of the quantitative research approach. The qualitative data analysis used in this research is descriptive qualitative data analysis. Because this qualitative data analysis describes what it is. Qualitative data analysis is used to process data from testing and evaluation results after this research is completed. The tools used in this research are based on SNI ISO 27005: 2022. The application of risk assessment for the Student Admission Information System is carried out in accordance with the guidelines in the SNI ISO 27005: 2022 document. The risk assessment process starts from risk identification, risk analysis, risk evaluation. The risk assessment process has been tested and successful. From the evaluation results, it shows that further research is needed which includes all information assets and other assets related to information security in the STT-NF New Student Admission Information System. The evaluation shows that further research covers*

*all information assets and other assets related to information security in the STT-NF New Student Admission Information System, the assessment needs to be carried out on the type of asset classification.*

*Key words: Risk assessment, SNI ISO 27005, SNI ISO 27001, information security risk, asset, security, hacking.*



STT - NF

## Daftar Isi

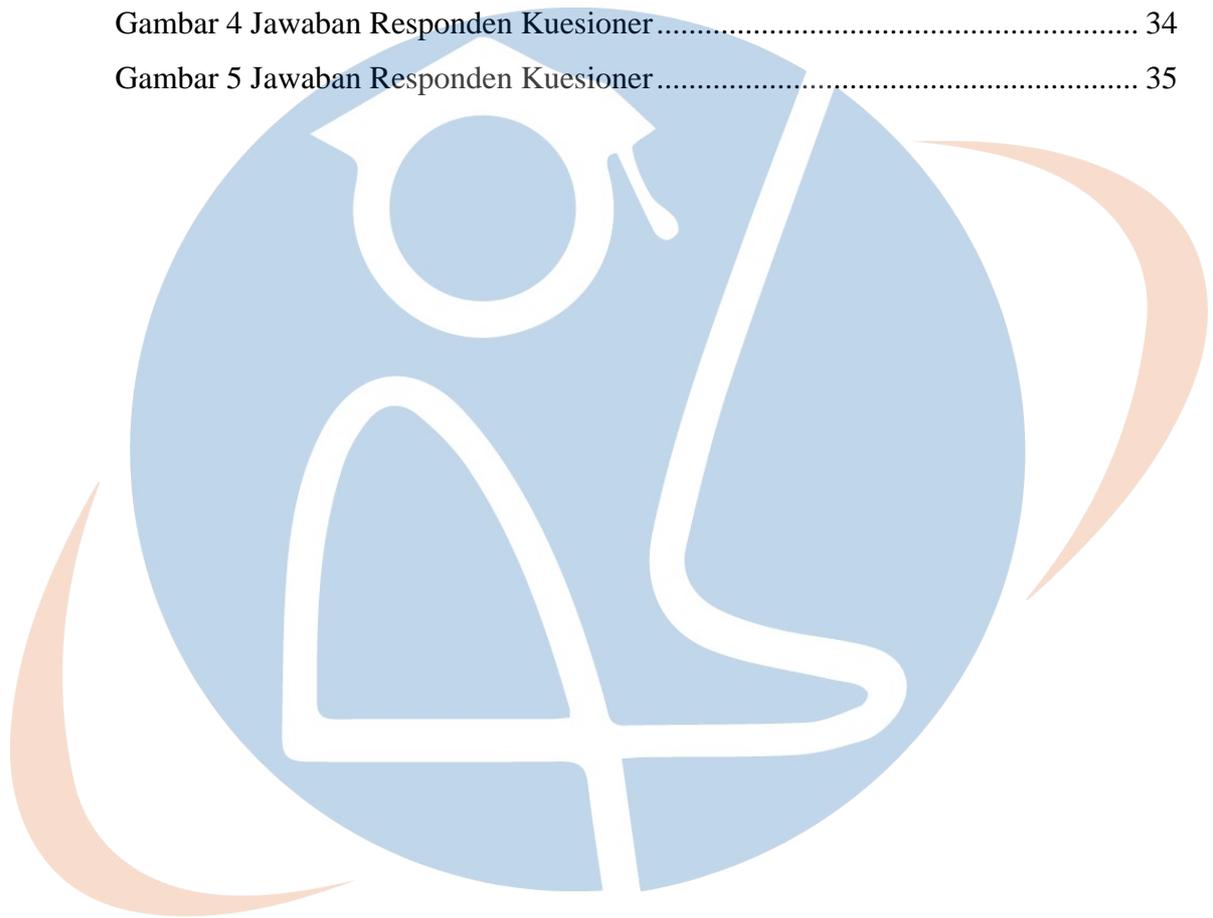
Halaman Pernyataan Orisinalitas .....	ii
Halaman Pengesahan .....	iii
Kata Pengantar .....	iv
Halaman Pernyataan Persetujuan .....	v
Abstrak .....	vi
Abstract .....	vii
Daftar Isi .....	ix
Daftar Gambar .....	xi
Daftar Tabel .....	xii
Bab I Pendahuluan .....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	2
1.3 Tujuan dan Manfaat Penelitian .....	2
1.4 Batasan Masalah .....	3
1.5 Sistematika Penulisan .....	3
Bab II Kajian Literatur .....	5
2.1 STT Terpadu Nurul Fikri .....	5
2.2 Sistem Informasi Penerimaan Mahasiswa .....	5
2.3 Sistem Manajemen Keamanan Informasi .....	6
2.3 International Standardization Organization .....	6
2.4 Penelitian Terkait .....	9
Bab III Metodologi Penelitian .....	13
3.1 Tahapan Penelitian .....	13
3.2 Rancangan Penelitian .....	15

3.2.1 Jenis Penelitian.....	15
3.2.2 Metode Analisis .....	15
3.2.3 Metode Pengumpulan Data.....	16
3.2.4 Lingkungan Pengembangan.....	16
3.2.5 Metode Implementasi.....	17
3.2.6 Metode Pengujian dan Evaluasi.....	17
Bab IV Implementasi dan Evaluasi.....	19
4.1 Studi Pendahuluan.....	19
4.2 Analisis Kebutuhan.....	21
4.3 Identifikasi Aset.....	22
4.4 Implementasi Asesmen Risiko.....	22
4.5 Evaluasi Hasil Asesmen Risiko.....	26
Bab V Kesimpulan dan Saran.....	29
5.1 Kesimpulan.....	29
5.2 Saran.....	30
Daftar Referensi.....	31
Lampiran.....	33

STT - NF

## Daftar Gambar

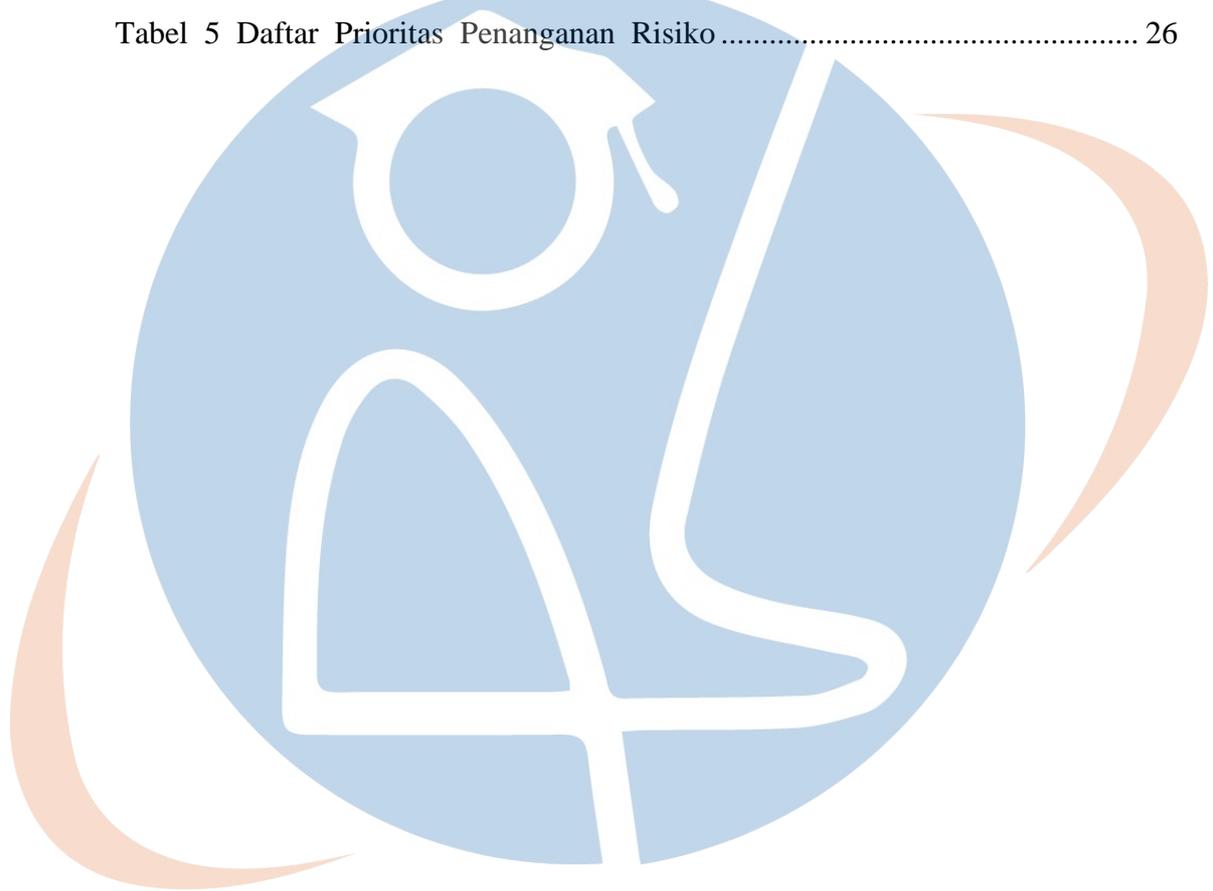
Gambar 1 Tahapan Penelitian .....	13
Gambar 2 Wawancara aset Sistem Informasi Penerimaan Mahasiswa .....	33
Gambar 3 Wawancara mengenai Sistem Informasi Penerimaan Mahasiswa .....	33
Gambar 4 Jawaban Responden Kuesioner .....	34
Gambar 5 Jawaban Responden Kuesioner .....	35



STT - NF

## Daftar Tabel

Tabel 1 Penelitian Terkait .....	9
Tabel 2 Identifikasi Aset .....	22
Tabel 3 Identifikasi Risiko .....	23
Tabel 4 Analisis Risiko .....	24
Tabel 5 Daftar Prioritas Penanganan Risiko .....	26



STT - NF

# Bab I

## Pendahuluan

### 1.1 Latar Belakang

Belakangan ini sistem manajemen keamanan informasi sedikit mendapat sorotan atas terjadinya gangguan layanan milik Bank Syariah Indonesia. Ada isu yang beredar alasan terjadi gangguan layanan Bank Syariah Indonesia di antaranya yaitu adanya serangan *ransomware* ke sistem server Bank Syariah Indonesia yang menyebabkan layanan milik Bank syariah tidak dapat berfungsi. Gangguan layanan ini berlangsung cukup lama namun setelah beberapa hari layanan Bank Syariah Indonesia mulai berangsur pulih [1]. Kejadian ini mengungkapkan bahwa perlunya mencegah terjadinya peretasan sebuah sistem oleh pihak yang tidak berkepentingan. Hal ini tertuang di pasal 6 dokumen SNI ISO 27001 yang berisi tindakan untuk menangani risiko dan peluang, asesmen risiko keamanan informasi, penanganan risiko keamanan informasi [2].

Sekolah Tinggi Teknologi Terpadu Nurul Fikri (juga dikenal sebagai STT-NF) adalah perguruan tinggi yang menggabungkan pengetahuan tentang teknologi informasi dengan pengembangan karakter, kepribadian, dan keterampilan Islami. STT-NF resmi didirikan pada tahun 2012 dengan Peraturan Menteri Pendidikan dan Kebudayaan Nomor 269/E/O/2012 [3]. Keamanan sistem informasi Sekolah Tinggi Teknologi Terpadu Nurul Fikri patut dipertanyakan karena belum diketahui apakah risiko keamanan informasi sistem yang dimiliki oleh Sekolah Tinggi Teknologi Terpadu sudah pernah dinilai atau belum.

Pendaftaran penerimaan mahasiswa di STT-NF dilaksanakan secara *online* melalui Sistem Informasi Penerimaan Mahasiswa. Pendaftaran dapat dilakukan dengan mengikuti panduan yang tersedia di situs kampus STT-NF pada bagian info pendaftaran penerimaan klik tombol admisi pendaftaran [4]. Memeriksa risiko keamanan sebuah situs

penting dilakukan karena untuk meminimalkan terjadi peretasan oleh pihak yang tidak mempunyai kepentingan dan mencegah terjadi kebocoran data pada sebuah situs.

Penelitian ini akan melakukan asesmen risiko keamanan informasi untuk mengidentifikasi ancaman potensial terhadap aset yang terkait dengan pemrosesan data serta menentukan cara terbaik untuk melindungi aset tersebut. Oleh sebab itu, penelitian ini diberi judul Asesmen Risiko Keamanan Informasi Sistem Informasi Penerimaan Mahasiswa pada STT-NF dengan SNI ISO/ IEC 27001:2022.

## **1.2 Rumusan Masalah**

Rumusan masalah pada penelitian ini sebagai berikut:

1. Bagaimana cara menyusun daftar aset informasi pada Sistem Informasi Penerimaan Mahasiswa?
2. Bagaimana cara melakukan asesmen risiko keamanan informasi pada Sistem Informasi Penerimaan Mahasiswa?
3. Bagaimana cara evaluasi hasil asesmen risiko keamanan informasi pada Sistem Informasi Penerimaan Mahasiswa?

## **1.3 Tujuan dan Manfaat Penelitian**

Tujuan penelitian ini sebagai berikut:

1. Memahami dan melaksanakan cara menyusun daftar aset informasi pada Sistem Informasi Penerimaan Mahasiswa.
2. Melaksanakan asesmen risiko pada Sistem Informasi Penerimaan Mahasiswa.
3. Melaksanakan proses evaluasi hasil asesmen risiko keamanan informasi pada Sistem Informasi Penerimaan Mahasiswa.

Manfaat yang akan didapat di antaranya:

1. Organisasi bisa menerapkan kebijakan mengenai risiko dari hasil penelitian ini sehingga keamanan informasi Sistem Informasi Penerimaan Mahasiswa menjadi lebih baik.
2. Peneliti mendapatkan pengetahuan dan pengalaman baru mengenai tahapan melaksanakan asesmen risiko keamanan informasi.

3. PMB menjadi lebih tenang karena Sistem Informasi Penerimaan Mahasiswa menjadi lebih aman sehingga tidak terjadi peretasan.
4. STT-NF dapat menggunakan hasil penelitian ini untuk mengetahui keamanan sistem informasi yang telah dibuat aman atau tidak.
5. STT-NF dapat menggunakan SNI ISO 27001:2022 ini untuk melakukan penanganan risiko atau menentukan sebuah keputusan.

#### **1.4 Batasan Masalah**

Penelitian ini dibatasi pada satu aset yaitu aset teknologi, karena data yang diperoleh tidak cukup. Penelitian ini dibatasi juga pada tahap asesmen risiko yang dilakukan karena tidak diperluas ke penanganan risiko. Aset yang diakses pada penelitian ini dibatasi pada aset teknologi. Penelitian ini tidak melakukan asesmen risiko pada semua aset yang ada karena keterbatasan waktu penelitian. Asesmen hanya dilakukan pada aset dengan klasifikasi teknologi karena data yang dibutuhkan untuk melakukan asesmen ke semua aset tidak cukup. Karena data yang digunakan untuk melakukan asesmen harus sesuai dengan data yang ada di Sistem Informasi Penerimaan Mahasiswa.

#### **1.5 Sistematika Penulisan**

Bab I Pendahuluan: Pendahuluan penelitian ini menghasilkan latar belakang yang berisi masalah yang ingin diselesaikan.

Bab II Kajian Literatur membahas teori pendukung yang digunakan penulis untuk Asesmen Risiko Keamanan Informasi Sistem Informasi Penerimaan Mahasiswa pada STT-NF dengan SNI ISO/ IEC 27001:2022.

Bab III Metodologi Penelitian membahas studi pendahuluan yang dilakukan, metode pengumpulan data yang digunakan untuk analisis kebutuhan, metode pengolahan data yang digunakan, metode pengujian yang digunakan, jenis penelitian yang digunakan pada penelitian ini.

Bab IV Implementasi dan Evaluasi: Implementasi penelitian ini menghasilkan seberapa besar tingkat risiko pada aset yang telah dilakukan asesmen, evaluasi hasil penelitian ini menghasilkan penilaian

yang telah dilakukan bagian penerimaan mahasiswa setelah asesmen dilakukan.

Bab V Kesimpulan dan Saran: Kesimpulan sesuai dengan tujuan dan hasil penelitian ini, saran untuk penelitian selanjutnya sebagai perbaikan atau pengembangan penelitian ini.



STT - NF

## **Bab II**

### **Kajian Literatur**

#### **2.1 STT Terpadu Nurul Fikri**

Sekolah Tinggi Teknologi Terpadu Nurul Fikri (juga disebut STT-NF) adalah perguruan tinggi yang didirikan pada tahun 2012 dengan Peraturan Menteri Pendidikan dan Kebudayaan Nomor 269/E/O/2012. STT-NF didirikan untuk “mendidik lulusan ilmu komputer yang berakhlak mulia, profesional, dan bersertifikat ilmu komputer [3].

STT-NF ingin menghasilkan generasi yang pintar dan bermoral. Setiap semester, mata kuliah keislaman dan kewirausahaan diberikan. Penelitian dilakukan di bagian “Penerimaan mahasiswa baru”. Bagian penerimaan mahasiswa baru terletak pada tab Waket III (Kemahasiswaan) di struktur organisasi STT-NF [3].

#### **2.2 Sistem Informasi Penerimaan Mahasiswa**

Sistem Informasi Penerimaan Mahasiswa ialah sistem yang dibuat oleh STT Nurul Fikri sebagai wadah penyelenggaraan penerimaan mahasiswa baru tahun 2023/2024 yang dilakukan secara daring. fungsi sistem ini yaitu diperuntukkan kepada mahasiswa baru untuk mendaftar kuliah di STT-NF. Fungsi sistem ini yaitu diperuntukkan kepada mahasiswa baru untuk mendaftar kuliah di STT-NF. Fitur di sistem ini ada 2 yaitu untuk calon mahasiswa reguler dan calon mahasiswa beasiswa. Fitur untuk calon mahasiswa reguler di antaranya bisa melihat status pendaftaran, bisa unggah berkas pendaftaran berupa data diri dan berkas akademik lainnya, bisa melihat status pendaftaran yang dilakukan sudah sampai tahap apa.

Fitur untuk calon mahasiswa beasiswa di antaranya unggah data diri lebih dari calon mahasiswa reguler, berkas surat rekomendasi dari rekanan / agen. tujuan: agar calon mahasiswa baru bisa daftar dari berbagai wilayah tanpa harus ke kampus. manfaat untuk calon mahasiswa akses yaitu bisa dilakukan dari berbagai daerah tanpa harus

ke kampus, pembayaran secara daring tanpa harus ke kampus. manfaat untuk pihak internal yaitu bisa merekap data dari calon mahasiswa baru mulai dari status tahapan yang sudah dilakukan, jika ada yang belum lengkap bisa di cek dan di tindak lanjut dengan menghubungi PMB STT-NF.

### **2.3 Sistem Manajemen Keamanan Informasi**

Untuk menjaga kelangsungan bisnis, meminimalkan risiko, dan mempercepat dan memaksimalkan keuntungan investasi dan peluang bisnis dengan menerapkan kebijakan keamanan informasi yang tepat, yang mencakup kebijakan, proses, dan struktur organisasi [5]. Audit keamanan informasi sangat penting untuk menjaga nilai informasi karena keamanan informasi sangat penting bagi bisnis saat ini, baik pemerintah maupun swasta. Dikenal juga sebagai Sistem Manajemen Keamanan Informasi (SMKI) atau "SMKI". Ini adalah disiplin ilmu yang digunakan untuk mengidentifikasi pemangku kepentingan penting yang mempengaruhi departemen keamanan atau organisasi. Ini dapat digunakan untuk melindungi informasi sebagai aset dan memastikan bahwa pemangku kepentingan lainnya tidak mengetahuinya [6].

### **2.3 International Standardization Organization**

Standar Nasional Indonesia (SNI) ISO/IEC 27001:2022, yang merupakan revisi dari SNI ISO/IEC 27001:2013, berjudul Teknologi informasi—Teknik keamanan—Keamanan informasi, keamanan siber, dan perlindungan privasi—Sistem manajemen keamanan informasi—Persyaratan, diterjemahkan ke dalam dua bahasa [2].

Komite Teknis 35-04, Keamanan Informasi, Keamanan Siber, dan Perlindungan Privasi, membuat standar ini. Standar ini dibahas dan disetujui pada pertemuan konsensus nasional di Depok pada tanggal 15 Februari 2023. Konsensus ini mempertemukan para pemangku kepentingan terkait, khususnya perwakilan produsen, konsumen dan konsumen pengguna, pakar, dan pemerintah. Standar ini menjalani masa komentar mulai 24 Februari 2023 hingga 10 Maret 2023, dan hasil akhirnya diadopsi menjadi SNI [2].

Karena manajemen risiko keamanan informasi tidak dapat dibatasi oleh pandangan sewenang-wenang atau restriktif tentang bagaimana risiko harus distrukturkan, digrupkan, diagregasikan, dipisahkan, atau dideskripsikan, sangat penting untuk mempertimbangkan risiko yang digabungkan secara terpisah untuk tujuan penganggaran manajemen risiko secara keseluruhan. Ini karena kontrol yang berbeda mungkin diperlukan untuk mengendalikannya.

Manajemen risiko keamanan informasi melibatkan analisis peristiwa dan dampaknya serta membuat keputusan tentang bagaimana dan kapan mengurangi risiko ke tingkat yang dapat diterima [7]. Manajemen risiko keamanan informasi biasanya mencakup penerapan kebijakan dan pengendalian keamanan yang tepat, meningkatkan kesadaran, dan mengevaluasi keberhasilan [5].

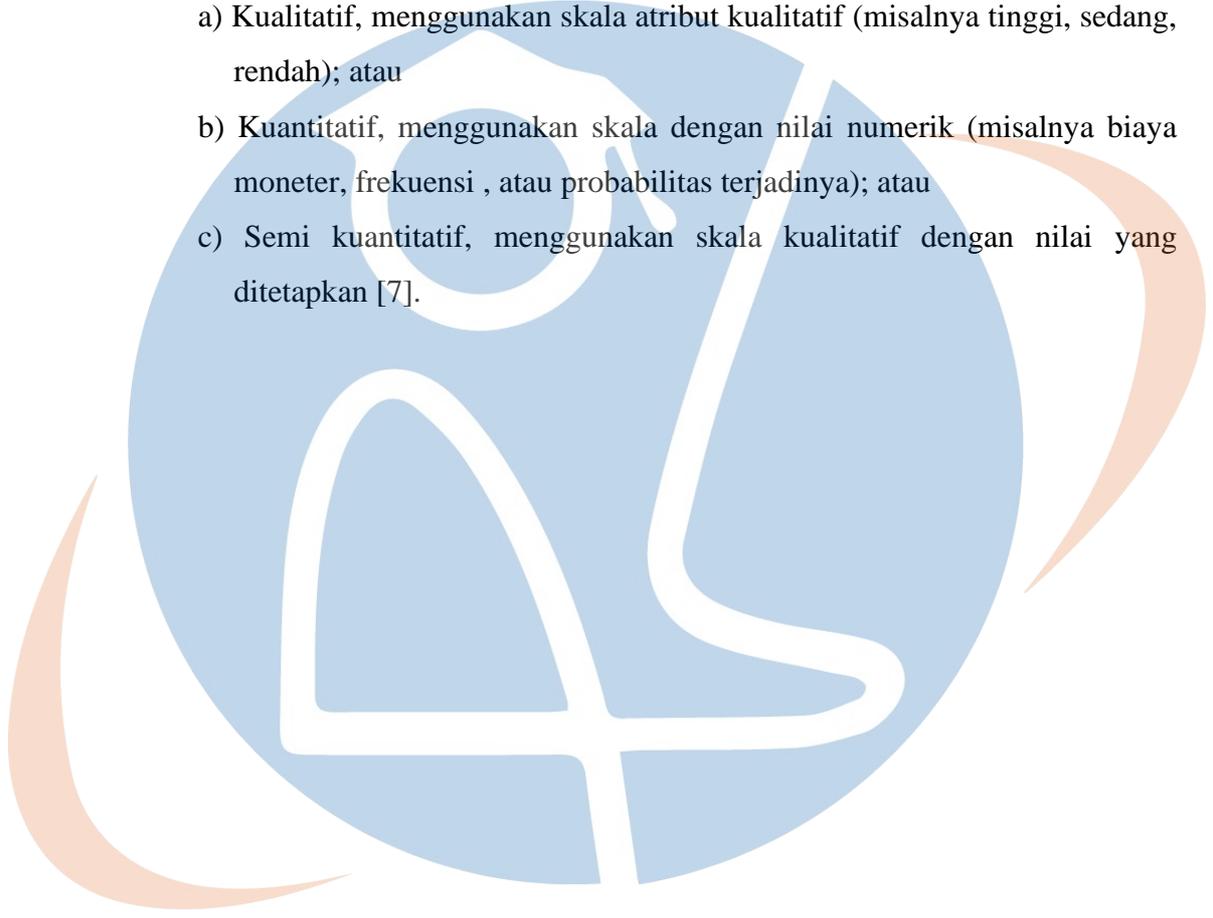
Risiko keamanan informasi dapat didefinisikan sebagai akibat dari ketidakpastian tentang sasaran keamanan informasi. Ketidakpastian ini biasanya dikaitkan dengan dampak negatif dari ketidakpastian pada sasaran keamanan informasi. Risiko keamanan informasi juga dapat dikaitkan dengan kemungkinan bahwa ancaman (3.1.9) akan memanfaatkan kerentanan (3.1.10) dari aset informasi atau kelompok aset informasi, sehingga menyebabkan kerugian bagi organisasi [7].

Total proses identifikasi risiko (3.2.4), analisis risiko (3.2.5), dan evaluasi risiko (3.2.6). Metode iteratif untuk melakukan asesmen risiko dapat meningkatkan kedalaman dan detail asesmen pada setiap pengulangan. Metode iteratif dalam evaluasi risiko dapat meningkatkan kedalaman dan detail evaluasi pada setiap pengulangan. Asesmen risiko memungkinkan pemilik risiko untuk memprioritaskan risiko yang sesuai dengan perspektif penanganan, terutama berdasarkan konsekuensi, kemungkinan, atau kriteria lain yang ditetapkan. Sejauh mungkin, hasil asesmen risiko harus konsisten, valid, dan dapat direplikasi, prosesnya sebaiknya didasarkan pada metode (lihat 6.5) dan alat yang dirancang dengan cukup detail [7]. ISO 31000 direferensikan dalam ISO/IEC 27001 sebagai model umum.

ISO/IEC 27001: 2022, 6.1.2, mensyaratkan bahwa untuk setiap risiko yang teridentifikasi, analisis risiko didasarkan pada penilaian terhadap akibat yang ditimbulkan oleh risiko tersebut dan penilaian terhadap kemungkinan terjadinya risiko untuk menentukan tingkat risiko. mempertaruhkan.

Teknik analisis risiko berdasarkan konsekuensi dan probabilitas dapat berupa:

- a) Kualitatif, menggunakan skala atribut kualitatif (misalnya tinggi, sedang, rendah); atau
- b) Kuantitatif, menggunakan skala dengan nilai numerik (misalnya biaya moneter, frekuensi, atau probabilitas terjadinya); atau
- c) Semi kuantitatif, menggunakan skala kualitatif dengan nilai yang ditetapkan [7].



STT - NF

## 2.4 Penelitian Terkait

Tabel berikut menunjukkan penelitian-penelitian terkait yang mempunyai kesamaan dengan penelitian ini. Ada tiga judul penelitian yang tersedia untuk perbandingan. Itu adalah karya muhammad bahrudin dan firmansyah, furqon mauladani, nurul fadhilah oktariza. Karena terdapat beberapa hubungan antara satu sama lain dalam bentuk pendekatan berdasarkan topik utamanya, maka penulis memanfaatkan ketiga kajian tersebut ketika menyusun makalah ini.

Tabel 1 Penelitian Terkait

No.	Nama dan Tahun	Judul	Subjek	Hasil
1	Muhammad Bahrudin dan Firmansyah, 2018	Manajemen Keamanan Informasi di Perpustakaan Menggunakan Framework SNI ISO/IEC 27001	Perpustakaan	Manajemen Keamanan Informasi di Perpustakaan berhasil diterapkan meskipun diterpa berbagai kendala.
2	Furqon Mauladani, 2017	Perancangan Sistem Manajemen Keamanan Informasi (Smki) Berdasarkan Sni Iso/Iec 27001:2022 Dan Sni Iso/Iec 27005:2022 (Studi Kasus Direktorat Pengembangan Teknologi Dan Sistem Informasi	Institut Teknologi Sepuluh Nopember	60 Resiko yang tidak diterima dari total 228 resiko yang telah teridentifikasi. Dari 60 resiko tersebut, terdapat 58 <i>risk modification</i> , 1 <i>risk avoidance</i> , dan 1 <i>risk sharing</i> . Tata kelola keamanan informasi yang dirancang berdasarkan SNI ISO/IEC 27001 adalah ruang lingkup SMKI, kebijakan SMKI, proses penilaian resiko, proses penanganan resiko, <i>statement of applicability</i> , dan sasaran

				keamanan informasi.
3	Nurul Fadhylah Oktariza, 2019	Analisis Sistem Manajemen Keamanan Informasi Menggunakan Standar ISO/IEC 27001 dan ISO/IEC 27002 Pada Kantor Pusat PT Jasa Marga	PT Jasa Marga	<i>Maturity level</i> ISO /IEC 27001 rata-rata berada di level satu dan <i>maturity level</i> ISO /IEC 27002 rata-rata berada di level dua, diharapkan hasil penelitian ini dapat membantu dan memberikan rekomendasi untuk kontrol keamanan yang dapat digunakan sebagai pedoman dan prosedur penerapan keamanan informasi.

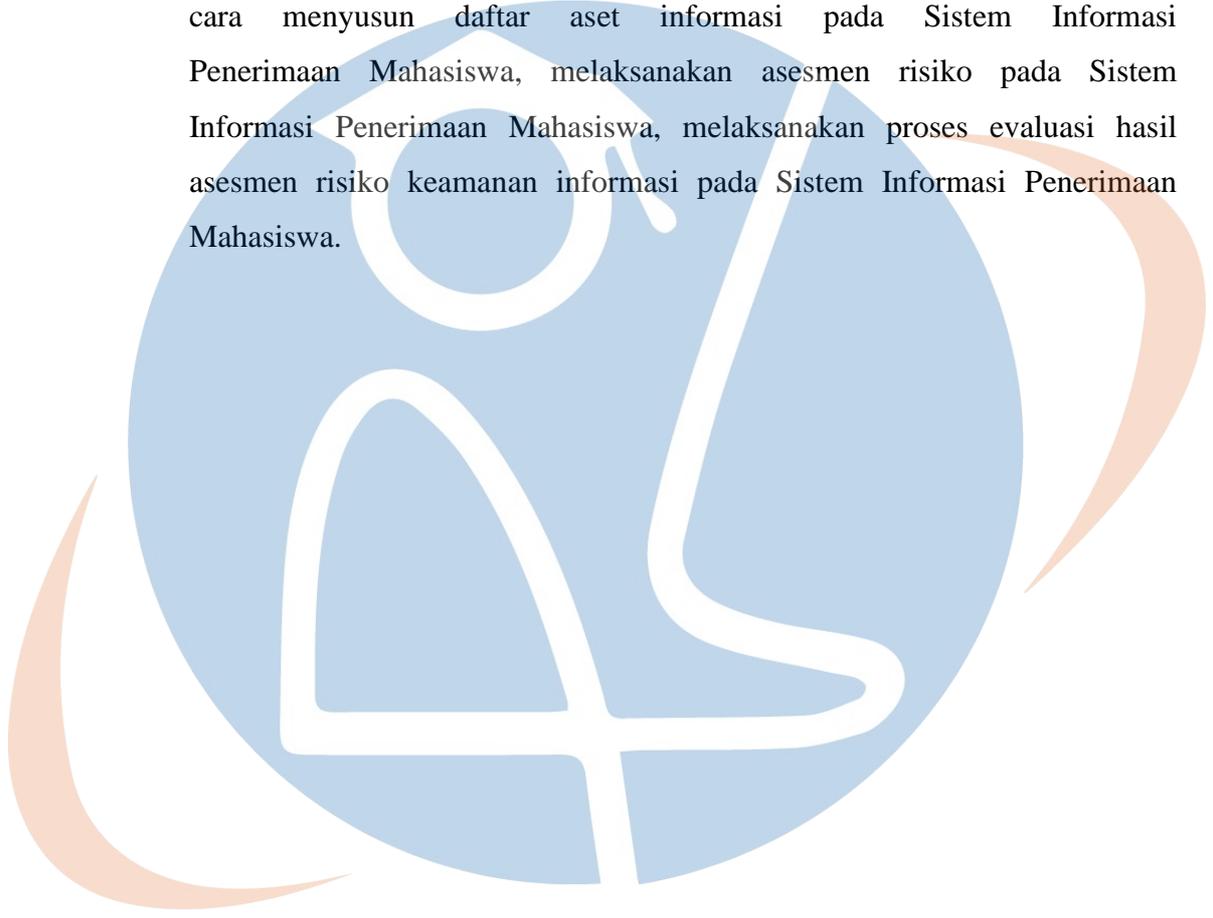
STT - NF

4	Abdullah Mumtaz, 2023	Asesmen Risiko Keamanan Informasi Sistem Informasi Penerimaan Mahasiswa pada STT-NF dengan SNI ISO/ IEC 27001:2022	Sistem Informasi Penerimaan Mahasiswa	
---	-----------------------	--	---------------------------------------	--

Persamaan / perbedaan penelitian terkait dengan penelitian ini. Pada penelitian pertama tahapan yang dilakukan yaitu melakukan manajemen keamanan informasi, *framework* yang digunakan yaitu SNI ISO 27001:2013. Pada penelitian kedua tahapan yang dilakukan yaitu melakukan manajemen risiko keamanan informasi berdasarkan SNI ISO/IEC 27005 dan perancangan dokumen SMKI berdasarkan SNI ISO/IEC 27001, asesmen risiko dilakukan di 4 bidang, asesmen risiko dilakukan oleh satu orang di setiap bidang, terdapat 1 metode pengumpulan data yang sama yaitu wawancara. Pada penelitian ketiga tahapan yang dilakukan yaitu analisis sistem menggunakan SNI ISO 27001 dan SNI ISO 27002, asesmen risiko dilakukan di berbagai divisi, penelitian dilakukan pada semua aset yang dimiliki, terdapat 2 metode penelitian pengumpulan data yang sama yaitu wawancara dan kuesioner. Pada penelitian ini penerapan hanya dilakukan pada asesmen risiko.

Tujuan penelitian terkait dengan penelitian. Pada penelitian pertama tujuan dilakukan penelitian meningkatkan kesadaran manajemen perpustakaan untuk mengamankan aset informasi yang dimiliki sehingga dapat diberdayakan sesuai dengan prinsip kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*). Pada penelitian kedua tujuan dilakukan penelitian mengidentifikasi, menganalisis dan mengevaluasi risiko yang dihadapi oleh DPTSI-ITS melalui manajemen risiko keamanan informasi berdasarkan SNI ISO/IEC 27005:2022, merancang tata kelola keamanan informasi yang berupa SMKI berdasarkan SNI ISO/IEC 27001:2022 yang dibutuhkan oleh DPTSI-ITS. Pada

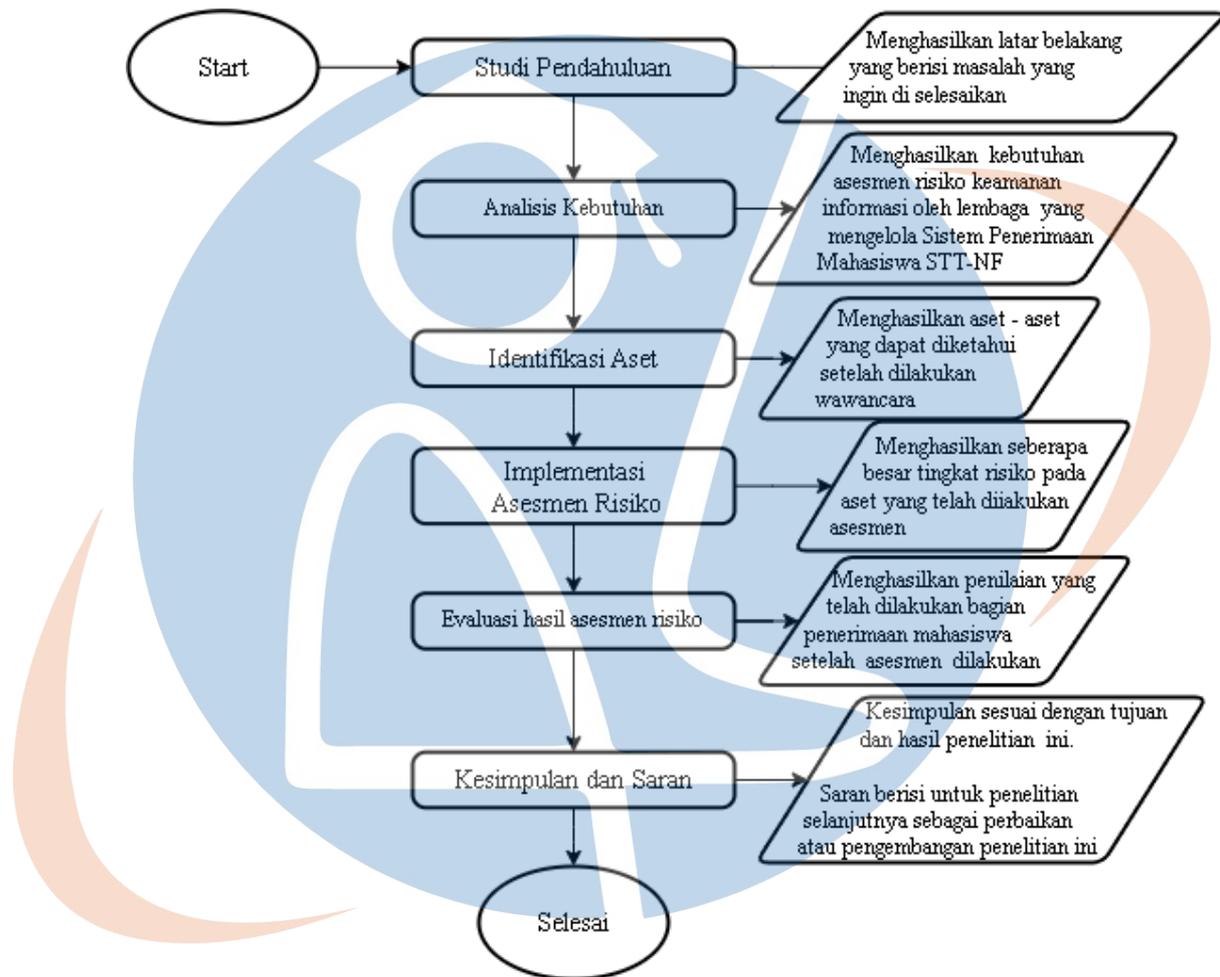
penelitian ketiga tujuan dilakukan penelitian menganalisis Standar Kebijakan Keamanan Informasi untuk menjaga sistem keamanan Web Portal Internal, menganalisis Manajemen Insiden Terkait Penyerangan Pada Web Portal Internal, menganalisis standar kebijakan terkait kapasitas kemampuan pegawai khususnya pada bagian keamanan informasi. Pada penelitian ini tujuan dilakukan penelitian memahami cara menyusun daftar aset informasi pada Sistem Informasi Penerimaan Mahasiswa, melaksanakan asesmen risiko pada Sistem Informasi Penerimaan Mahasiswa, melaksanakan proses evaluasi hasil asesmen risiko keamanan informasi pada Sistem Informasi Penerimaan Mahasiswa.



STT - NF

## Bab III Metodologi Penelitian

### 3.1 Tahapan Penelitian



Gambar 1 Tahapan Penelitian

Berikut ini penjelasan setiap tahapan penelitian pada gambar diagram penelitian di atas:

#### 1. Studi Pendahuluan

Studi pendahuluan yang dilakukan yaitu membaca literatur SNI ISO 27001 dan SNI ISO 27005, membaca hasil penelitian orang lain, membaca literatur metode penelitian.

## **2. Analisis Kebutuhan**

Analisis kebutuhan yang telah dilakukan yaitu pengumpulan data melalui wawancara dan menghasilkan keluaran berupa kebutuhan asesmen risiko.

## **3. Identifikasi Aset**

Identifikasi aset yang dilakukan yaitu pengumpulan data aset apa saja yang dapat diketahui setelah melakukan wawancara dan mengklasifikasikan aset yang sudah diketahui.

## **4. Implementasi Asesmen Risiko**

Implementasi dilakukan untuk mengidentifikasi kelemahan, ancaman, dan efek ancaman yang merugikan serta menilai kemungkinan gangguan dan dampak yang terjadi. Identifikasi risiko, analisis penentuan tingkat risiko, dan evaluasi risiko adalah beberapa langkah yang dilakukan selama asesmen risiko.

## **5. Evaluasi Hasil Asesmen Risiko**

Evaluasi hasil asesmen risiko yang dilakukan yaitu bagian penerimaan mahasiswa baru memberikan penilaian terhadap pelaksanaan asesmen risiko yang akan digunakan untuk penanganan risiko dan implementasi SMKI.

## **6. Kesimpulan dan Saran**

Hasil yang diharapkan adalah bahwa bagian penerimaan mahasiswa harus melakukan asesmen risiko secara berkala untuk mengetahui risiko apa yang dapat terjadi dan cara mengatasi risiko tersebut. Penelitian selanjutnya diharapkan dapat melakukan asesmen risiko menyeluruh terhadap setiap elemen sistem informasi penerimaan mahasiswa.

## 3.2 Rancangan Penelitian

### 3.2.1 Jenis Penelitian

Penelitian tindakan (*action research*) ini bertujuan untuk menerapkan SMKI dalam proses evaluasi risiko organisasi, yaitu bagian penerimaan mahasiswa baru STT-NF. Hasil penelitian ini mencakup nilai risiko untuk setiap aset informasi dan aset lain yang berkaitan dengan keamanan informasi, serta saran untuk penanganan risiko untuk aset dengan nilai risiko sedang dan tinggi. Emosional dan dekat antara subjek penelitian dan peneliti.

### 3.2.2 Metode Analisis

Menurut Kuncoro (2013), data kuantitatif adalah data yang diukur dalam skala numerik atau angka. Mereka juga disebut sebagai data interval dan data rasio. Metode penelitian kuantitatif menghasilkan data yang lebih dapat diukur, jadi mereka tidak memperlakukan hubungan emosional dan intim antara peneliti dan subjek penelitian karena hasil penelitian lebih banyak tergantung pada instrumen dan variabel yang diukur daripada hubungan antara mereka [8].

Proses analisis data secara kuantitatif dalam asesmen risiko digunakan dalam 3 tahap. Metode kuantitatif digunakan dengan cara memberi nilai angka untuk peluang terjadinya gangguan keamanan, dampak kerugian jika gangguan keamanan terjadi, dan level risikonya diperoleh dari hasil perkalian peluang terjadinya gangguan keamanan dikali dengan dampak kerugian jika gangguan keamanan terjadi. Data yang dianalisis dengan kuantitatif adalah data aset yang dimiliki Sistem Informasi Penerimaan Mahasiswa. Analisis data yang diperlukan dilakukan melalui metode survei, yang merupakan bagian dari pendekatan penelitian kuantitatif [9].

Data kualitatif adalah data yang tidak dapat diukur dalam skala numerik. Data kualitatif di penelitian ini diperoleh dari hasil penyebaran kuesioner dan hasil wawancara. Analisis data kualitatif yang digunakan dalam penelitian ini adalah analisis data kualitatif

deskriptif. Karena analisis data kualitatif ini menguraikan secara apa adanya. Analisis data kualitatif digunakan untuk mengolah data hasil pengujian dan evaluasi setelah penelitian ini selesai dilakukan. Proses analisis data secara kualitatif dilakukan dengan mengacu pada teori-teori yang digunakan dalam penelitian ini di antaranya teori asesmen risiko di SNI ISO 27001, teori asesmen risiko di SNI ISO 27005.

### **3.2.3 Metode Pengumpulan Data**

Peneliti menggunakan metode kuesioner untuk mengumpulkan data. Data awal yang digunakan dalam penelitian ini adalah data yang telah dikumpulkan sebelumnya untuk tujuan penelitian. Data penelitian ini diperoleh menggunakan 2 metode yaitu wawancara dan kuesioner. Wawancara dilakukan ke bagian penerimaan mahasiswa baru untuk memperoleh data yang dibutuhkan untuk melakukan asesmen risiko. Kuesioner digunakan untuk evaluasi hasil asesmen risiko. Kuesioner dilakukan ke bagian penerimaan mahasiswa dan LTSI bagian sistem informasi setelah penulis memberikan hasil penilaian dan rekomendasi kepada bagian penerimaan mahasiswa [10].

Informasi yang dikumpulkan terdiri dari jawaban atas pertanyaan peneliti. Kuesioner ialah teknik pengumpulan data di mana serangkaian pertanyaan atau pernyataan tertulis diberikan kepada responden. Kuesioner yang dibuat terdiri atas pertanyaan yang berhubungan dengan kegiatan yang akan dilakukan di penelitian ini. Kegiatan yang akan dilakukan pada penelitian ini yaitu asesmen risiko, pertanyaan yang ada di kuesioner evaluasi berisi pertanyaan umum ketika penelitian selesai dilakukan. Kuesioner pada penelitian ini digunakan untuk evaluasi setelah penelitian ini selesai.

### **3.2.4 Lingkungan Pengembangan**

Penelitian ini dilakukan di STT Terpadu Nurul Fikri yang beralamat di Jl. Raya Lenteng Agung No.20-21, RT.4/RW.1, Srengseng Sawah, Kec. Jagakarsa, Jakarta Selatan.

Alat dan bahan yang digunakan dalam penelitian ini:

1. Laptop HP 14an400au
  - Tipe Prosesor: AMD A8
  - Ram 12.00 GB
  - Sistem Operasi: Windows 10

2. *Software* yang digunakan

- *Draw.Io*
- *Google form*
- *Google Docs*
- *Microsoft Word*
- *Microsoft Excel*

Narasumber yang menjadi objek penelitian yaitu humas bagian penerimaan mahasiswa baru STT-NF

### **3.2.5 Metode Implementasi**

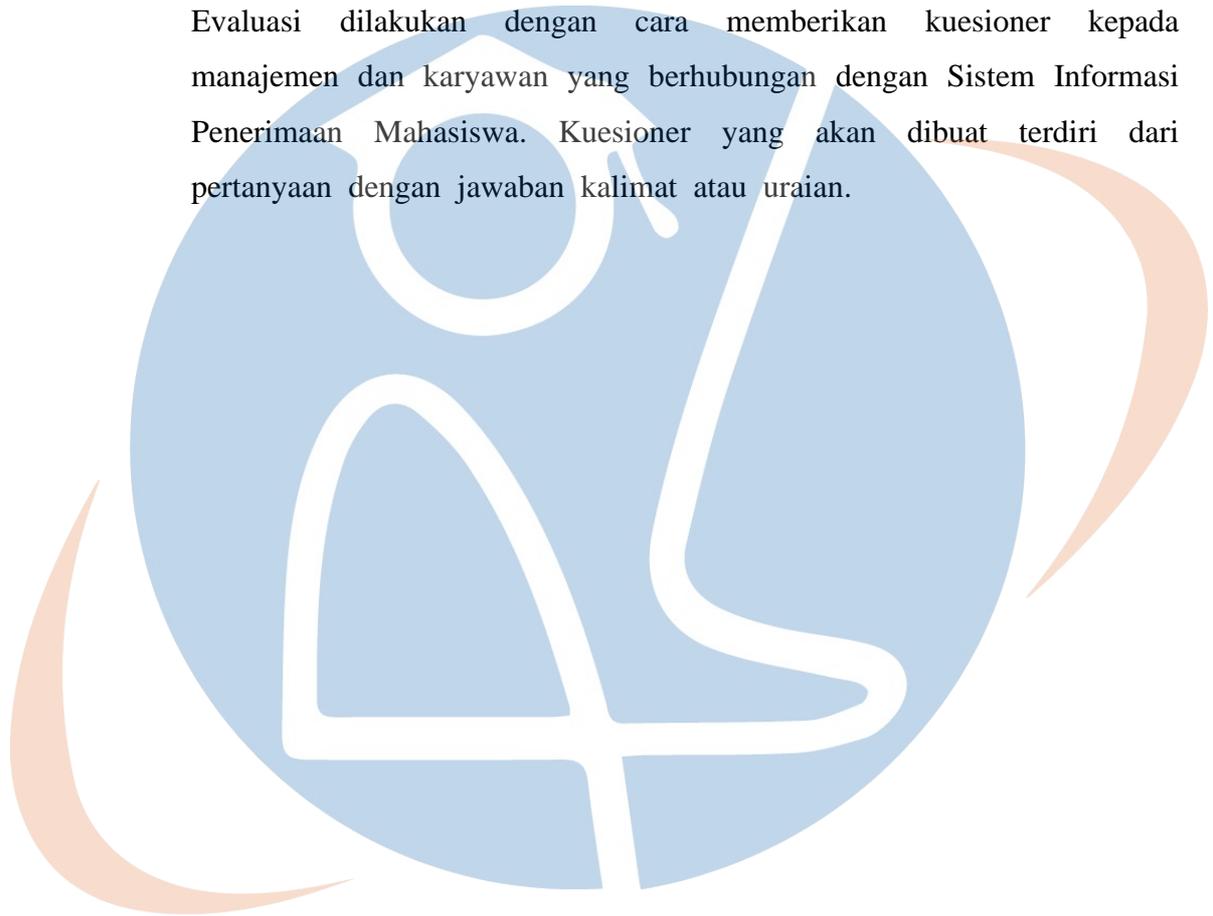
Menerapkan asesmen risiko dengan *framework* di SNI ISO 27001:2022 dan 27005:2022, proses asesmen risiko dimulai dengan identifikasi risiko (daftar aset), analisis risiko (nilai atau level risiko), evaluasi risiko (penentuan prioritas penanganan risiko yang direkomendasikan). Identifikasi risiko dilakukan dengan membuat daftar aset dan melakukan klasifikasi berdasarkan Lampiran a pada dokumen SNI ISO 27005. Analisis risiko dilakukan dengan menilai risiko berdasarkan 4 kategori yaitu rendah, sedang, tinggi, sangat tinggi. Nilai dalam analisis risiko memiliki rentang nilai 0 sampai 25. Nilai tersebut didapat dari hasil perkalian antara dampak dan kemungkinan. Nilai dampak adalah 0, 1, 2, 3, 4, 5 dan nilai kemungkinan risiko adalah 0, 1, 2, 3, 4, 5. Evaluasi risiko dilakukan dengan menentukan prioritas penanganan yang direkomendasikan.

### **3.2.6 Metode Pengujian dan Evaluasi**

Dalam penelitian ini, UAT (*User Acceptance Test*) digunakan untuk mengetahui apakah asesmen sudah sesuai harapan atau belum. Pengujian dilakukan sendiri oleh penulis dengan cara mengecek apakah hasil asesmen sudah sesuai dengan teori dan rencana. Proses

pengujian dalam penelitian ini menggunakan UAT. UAT dalam penelitian ini digunakan untuk evaluasi hasil asesmen risiko. Evaluasi hasil asesmen risiko dilakukan untuk mengecek hasil asesmen sudah sesuai dengan teori dan rencana atau belum, dan memberikan rekomendasi aset yang diprioritaskan untuk ditangani kepada perusahaan.

Evaluasi adalah proses terakhir dari seluruh proses penelitian. Evaluasi dilakukan dengan cara memberikan kuesioner kepada manajemen dan karyawan yang berhubungan dengan Sistem Informasi Penerimaan Mahasiswa. Kuesioner yang akan dibuat terdiri dari pertanyaan dengan jawaban kalimat atau uraian.



STT - NF

## **Bab IV**

### **Implementasi dan Evaluasi**

Bab 4 ini akan membahas mengenai hasil studi pendahuluan yang telah dilakukan, uraian hasil wawancara dengan bagian penerimaan mahasiswa baru STT-NF, tahapan implementasi asesmen risiko yang telah dilakukan, evaluasi hasil penelitian secara keseluruhan

#### **4.1 Studi Pendahuluan**

Semua teori telah dipelajari mulai dari teori SNI ISO 27001:2022, teori SNI ISO 27005:2022, teori pengolahan data menggunakan metode kuantitatif, teori pengolahan data menggunakan metode kualitatif, penelitian terkait untuk menyelesaikan masalah di rumusan masalah hingga tujuan - tujuan di penelitian ini tercapai. Tahapan kedua yang akan dilakukan yaitu memahami kebutuhan organisasi. Kebutuhan organisasi didapatkan melalui wawancara dengan bagian penerimaan mahasiswa baru. Organisasi harus memiliki proses penilaian risiko keamanan informasi berikut:

1. Menentukan dan memelihara standar risiko keamanan informasi, termasuk standar toleransi risiko dan praktik penilaian risiko keamanan informasi.
2. Ulangi penilaian risiko keamanan informasi untuk memastikan hasil yang konsisten, valid, dan dapat dibandingkan.
3. Identifikasi risiko keamanan informasi dengan menerapkan proses penilaian risiko keamanan informasi untuk mengidentifikasi risiko yang terkait dengan hilangnya kerahasiaan, integritas, dan ketersediaan informasi dalam sistem manajemen keamanan informasi.
4. Identifikasi pemilik risiko.
5. Menganalisis risiko keamanan informasi dengan mengevaluasi potensi dampak jika risiko yang diidentifikasi pada langkah 1 terjadi.

Teks tersebut dapat disingkat menjadi: Mengidentifikasi risiko dan menilai kemungkinan realistis terjadinya risiko pada 6.1. Singkatan dalam teks ini: Penentuan tingkat risiko, penilaian risiko keamanan informasi, dan perbandingan hasil analisis risiko dengan kriteria risiko yang telah ditetapkan. Untuk mempersingkat teks, Anda dapat menggunakan kata-kata berikut:

- 1) Memprioritaskan risiko yang dianalisis untuk manajemen risiko.
- 2) Organisasi harus memelihara informasi terdokumentasi mengenai proses penilaian risiko keamanan informasinya. Teks ini telah dipersingkat.

Organisasi harus menyimpan data asesmen risiko keamanan informasi dengan mempertimbangkan kriteria dalam 6.1 dan melakukannya secara berkala atau saat ada perubahan yang signifikan. memperpendek teks [2]

Untuk mengidentifikasi dampak dan prioritas dari insiden keamanan informasi, seharusnya ada kesepakatan mengenai metode kategorisasi dan prioritas insiden. Titik kontak harus melakukan penilaian terhadap setiap peristiwa yang berkaitan dengan keamanan informasi dengan menggunakan strategi yang disepakati. Hasil dan keputusan asesmen harus dicatat secara menyeluruh untuk referensi dan verifikasi di masa mendatang [11].

Untuk menentukan signifikansi risiko berdasarkan konsekuensi, kemungkinan, dan tingkat risiko, kriteria asesmen risiko digunakan. Persepsi dan ekspektasi pihak yang berkepentingan sesuai dengan standar risiko organisasi. Organisasi harus menggunakan proses asesmen risiko organisasi identifikasi risiko, yang merupakan proses untuk menemukan, merekognisi, dan mendeskripsikan risiko analisis risiko, yang merupakan proses untuk memahami jenis risiko dan tingkat risiko. Proses asesmen risiko harus didasarkan pada metode dan alat yang dirancang dengan cukup detail untuk memastikan bahwa hasilnya konsisten, valid, dan dapat direplikasi. Selain itu, hasilnya

harus dapat direplikasi secara akurat sehingga dapat digunakan kembali di masa depan.

Untuk memenuhi persyaratan yang ditetapkan dalam ISO/IEC 27001:2022, 6.1.2, ISO/IEC 27001 tidak menetapkan metode khusus yang harus digunakan. Proses evaluasi risiko keamanan informasi, seperti yang dijelaskan dan diterapkan dalam ISO/IEC 27001:2022, 6.1, harus dimasukkan ke dalam operasi organisasi. Ini harus dilakukan pada interval yang direncanakan atau ketika perubahan yang signifikan diusulkan atau terjadi. Sebaiknya interval asesmen risiko sesuai dengan SMKI [7].

#### **4.2 Analisis Kebutuhan**

Analisis kebutuhan sudah dilakukan melalui wawancara. Hasil wawancara diperoleh data yang dibutuhkan untuk melakukan asesmen risiko, mulai dari aset yang ada di Sistem Informasi Penerimaan Mahasiswa sampai aset yang akan dilakukan asesmen risiko. Ada lima aset yang dimiliki. Yang pertama teknologi penunjang. Teknologi penunjang yang digunakan oleh Sistem Informasi Penerimaan Mahasiswa yaitu *cloud base*. Yang kedua teknologi pengolahan data. Teknologi pengolahan data yang digunakan Sistem Informasi Penerimaan mahasiswa yaitu *spreadsheet*. Yang ketiga sdm. Aset sdm ini terdiri dari 2 orang pengelola informasi PMB, 1 orang *marketing*, 2 orang pengelola desain. Yang keempat laptop atau *pc (personal computer)*. Laptop atau *pc (personal computer)* yang digunakan pegawai bidang PMB ada 5. Laptop atau *pc (personal computer)* pegawai bidang PMB yang menggunakan *spreadsheet* ada 5. Laptop atau *pc (personal computer)* pegawai PMB yang mengakses sistem PMB ada 3. Yang kelima sistem operasi. Sistem operasi yang dijalankan pada laptop atau *pc (personal computer)* pegawai bidang PMB menggunakan sistem operasi *windows 11*. Hasil analisis kebutuhan diperoleh peneliti melalui proses identifikasi aset, identifikasi risiko, analisis risiko, evaluasi risiko. Metode pengolahan di tahap analisis kebutuhan ini menggunakan metode kualitatif, metode kualitatif di tahap analisis

kebutuhan ini digunakan dengan cara mengaitkan hasil wawancara dengan teori-teori yang ada. Hasil wawancara yang tertera di atas sudah sesuai dengan kebutuhan asesmen risiko di SNI ISO 27001:2022 pasal 4 tentang rencana asesmen dan metode asesmen.

### 4.3 Identifikasi Aset

Ruang lingkup aset yang dikelola informasi dan akan di nilai risiko yaitu pada aset *cloud base*, *spreadsheet*, sistem operasi dengan jenis aset teknologi. Hal ini ditentukan berdasarkan data hasil wawancara dengan bagian penerimaan mahasiswa baru. Tahapan identifikasi aset diperoleh melalui hasil wawancara dengan bagian penerimaan mahasiswa baru. Setelah diperoleh data aset hasil wawancara diklasifikasikan berdasarkan Lampiran a pada dokumen SNI ISO 27005. Hasil proses identifikasi aset dirangkum dalam tabel 2 identifikasi aset.

Tabel 2 Identifikasi Aset

No.	Nama Aset	Jenis Aset	Pemilik	Bagian
1.	<i>Cloud Base</i>	Teknologi	STT-NF	PMB
2.	<i>Spreadsheet</i>	Teknologi	STT-NF	PMB
3.	Pengelola Informasi PMB	Orang	STT-NF	PMB
4.	<i>Marketing</i>	Orang	STT-NF	<i>Marketing</i>
5.	Pengelola Desain	Orang	STT-NF	Desain
6.	Laptop / Pc	Fisik	STT-NF	PMB
7.	Sistem Operasi	Teknologi	STT-NF	PMB

### 4.4 Implementasi Asesmen Risiko

Pada tahap implementasi asesmen risiko ini ada tiga proses yang dilakukan yaitu identifikasi risiko, analisis risiko, evaluasi risiko. Identifikasi risiko yaitu memberikan nilai tiap aset dari sisi dampak jika

terjadi gangguan (*severity*) dan kemungkinan (*likelihood*). Nilai kemungkinan dan dampak terjadi gangguan ditentukan berdasarkan hasil wawancara dengan bagian penerimaan mahasiswa baru.

### 1. Identifikasi Risiko

Dari daftar aset yang dihasilkan pada tahapan identifikasi aset disusun tabel untuk memberi nilai kemungkinan dan nilai dampak pada setiap aset yang ada. Tahapan identifikasi risiko ini menggunakan metode kuantitatif. Metode kuantitatif digunakan dengan cara memberi nilai kemungkinan dan nilai dampak pada setiap aset. Hasil identifikasi risiko dirangkum dalam tabel 3 identifikasi risiko.

Tabel 3 Identifikasi Risiko

No.	Nama Aset	Klasifikasi Aset	Vulnerability	Threat	Impact	Kemungkinan	Dampak jika terjadi gangguan
1.	<i>Cloud Base</i>	Teknologi	Terlalu mempercayai keamanan pada <i>cloud</i> sistem yang digunakan oleh <i>cloud base</i>	Pernah mengalami <i>down</i> ketika banyak yang mengakses, Sistem sering digunakan calon mahasiswa baru untuk coba-coba seperti coba masuk, coba daftar dan sebagainya	Sistem tidak dapat diakses hingga perbaikan selesai dilakukan.	4	3
2.	<i>Spreadsheet</i>	Teknologi	Tidak ada karena akses dibatasi oleh organisasi sehingga yang memiliki akses hanya yang di <i>invite</i> oleh organisasi	Tidak ada, karena keamanan yang diterapkan cukup ketat	C: data digunakan untuk kebutuhan yang tidak seharusnya. Catatan: Belum pernah terjadi	0	0

3.	Sistem Operasi	Teknologi	Terdapat <i>bug</i> yang dapat dieksploitasi oleh penyerang dan <i>malware</i> dapat diinstal pada perangkat pengguna	Memungkinkan penyerang menginstal <i>malware</i> tanpa interaksi pengguna	Mengakibatkan terganggunya kerahasiaan, integritas dan ketersediaan sistem	4	4
----	----------------	-----------	---	---	--	---	---

## 2. Analisis Risiko

Data pada proses analisis risiko ini didapatkan dari proses identifikasi risiko. Metode yang digunakan pada proses analisis risiko ini adalah kuantitatif. Metode kuantitatif digunakan dengan mengalikan nilai dampak dan nilai gangguan pada setiap aset. Proses identifikasi risiko adalah proses untuk mengidentifikasi risiko - risiko pada setiap aset yang dimiliki. Proses menentukan kriteria penilaian risiko adalah dengan mengalikan kemungkinan dan dampak. Nilai dalam analisis risiko memiliki rentang nilai 0 sampai 25. Nilai dampak adalah 0, 1, 2, 3, 4, 5 dan nilai kemungkinan adalah 0, 1, 2, 3, 4, 5. Proses menentukan kriteria rendah, sedang, tinggi, sangat tinggi ditentukan dari hasil perkalian dampak dan kemungkinan. Nilai rendah memiliki rentang nilai 0 sampai 4. Nilai sedang memiliki rentang nilai 5 sampai 9. Nilai tinggi memiliki rentang nilai 10 sampai 16. Nilai sangat tinggi memiliki rentang nilai 16 sampai 25. Hasil analisis risiko dirangkum dalam tabel 4 analisis risiko.

Tabel 4 Analisis Risiko

No	Nama Aset	Klasifikasi Aset	Vulnerability	Threat	Impact	Kemungkinan	Dampak jika terjadi gangguan	Nilai Risiko dalam angka	Nilai Risiko dalam teks
----	-----------	------------------	---------------	--------	--------	-------------	------------------------------	--------------------------	-------------------------

1.	<i>Cloud Base</i>	Teknologi	Terlalu mempercayai keamanan pada <i>cloud</i> sistem yang digunakan oleh <i>cloud base</i>	Pernah mengalami <i>down</i> ketika banyak yang mengakses, Sistem sering digunakan calon mahasiswa baru untuk coba-coba seperti coba masuk, coba daftar dan sebagainya	Sistem tidak dapat diakses hingga perbaikan selesai dilakukan	4	3	12	Tinggi
2.	<i>Spreadsheet</i>	Teknologi	Tidak ada karena akses dibatasi oleh organisasi sehingga yang memiliki akses hanya yang di <i>invite</i> oleh organisasi	Tidak ada, karena keamanan yang diterapkan cukup ketat	C: data digunakan untuk kebutuhan yang tidak seharusnya. Catatan: Belum pernah terjadi	0	0	0	Rendah
3.	Sistem Operasi	Teknologi	Terdapat <i>bug</i> yang dapat dieksploitasi oleh penyerang dan <i>malware</i> dapat diinstal pada perangkat pengguna	Memungkinkan penyerang menginstal <i>malware</i> tanpa interaksi pengguna	Mengakibatkan terganggunya kerahasiaan, integritas dan ketersediaan sistem	4	4	16	Tinggi

### 3. Evaluasi Risiko

Evaluasi risiko dilakukan dengan 2 tahap yaitu cek asesmen risiko sudah sesuai dengan teori dan rencana atau belum, memberi rekomendasi aset yang diprioritaskan untuk ditangani kepada perusahaan. Evaluasi risiko dilakukan sendiri oleh penulis. Evaluasi risiko dapat dimulai setelah nilai risiko setiap aset pada proses analisis risiko diketahui. Evaluasi risiko sudah selesai dilakukan dan sudah sesuai dengan teori dan rencana. Penulis memberikan rekomendasi kepada perusahaan agar aset teknologi yaitu sistem operasi dan *cloud base* diprioritaskan untuk ditangani karena nilai risiko yang dihasilkan tinggi sehingga harus dilakukan penanganan agar nilai risiko yang dihasilkan menjadi rendah. Metode yang digunakan pada proses evaluasi risiko ini adalah kualitatif. Metode kualitatif digunakan dengan cara menghubungkan hasil asesmen pada teori yang digunakan pada penelitian ini. Hasil evaluasi risiko dirangkum dalam tabel 5 daftar prioritas penanganan risiko. Isi tabel daftar prioritas penanganan risiko didapat dari hasil analisis risiko. Makna dari aset yang terdapat di tabel daftar prioritas penanganan risiko yaitu aset yang memiliki nilai risiko tinggi. Oleh sebab itu prioritas penanganan risiko diberikan agar aset yang memiliki nilai risiko tinggi berkurang sehingga menjadi rendah.

Tabel 5 Daftar Prioritas Penanganan Risiko

No.	Nama Aset	Klasifikasi Aset	Prioritas Penanganan
1.	Sistem Operasi	Teknologi	1
2.	<i>Cloud Base</i>	Teknologi	2

#### 4.5 Evaluasi Hasil Asesmen Risiko

Proses UAT dilakukan kepada dua pengguna hasil asesmen risiko. Evaluasi hasil asesmen risiko ini adalah evaluasi keseluruhan hasil skripsi yang telah dibuat oleh penulis. Evaluasi dilakukan dengan

memberikan kuesioner kepada dua orang. Metode analisis pada tahapan evaluasi ini adalah kualitatif. Kuesioner dibuat menggunakan platform *google form*, kuesioner terdiri dari pertanyaan dengan jawaban penjelasan singkat. Kuesioner sudah selesai disebar, kriteria responden kuesioner ini adalah mengetahui proses penelitian yang sedang dilakukan, mengetahui SMKI yang diterapkan pada penelitian ini.

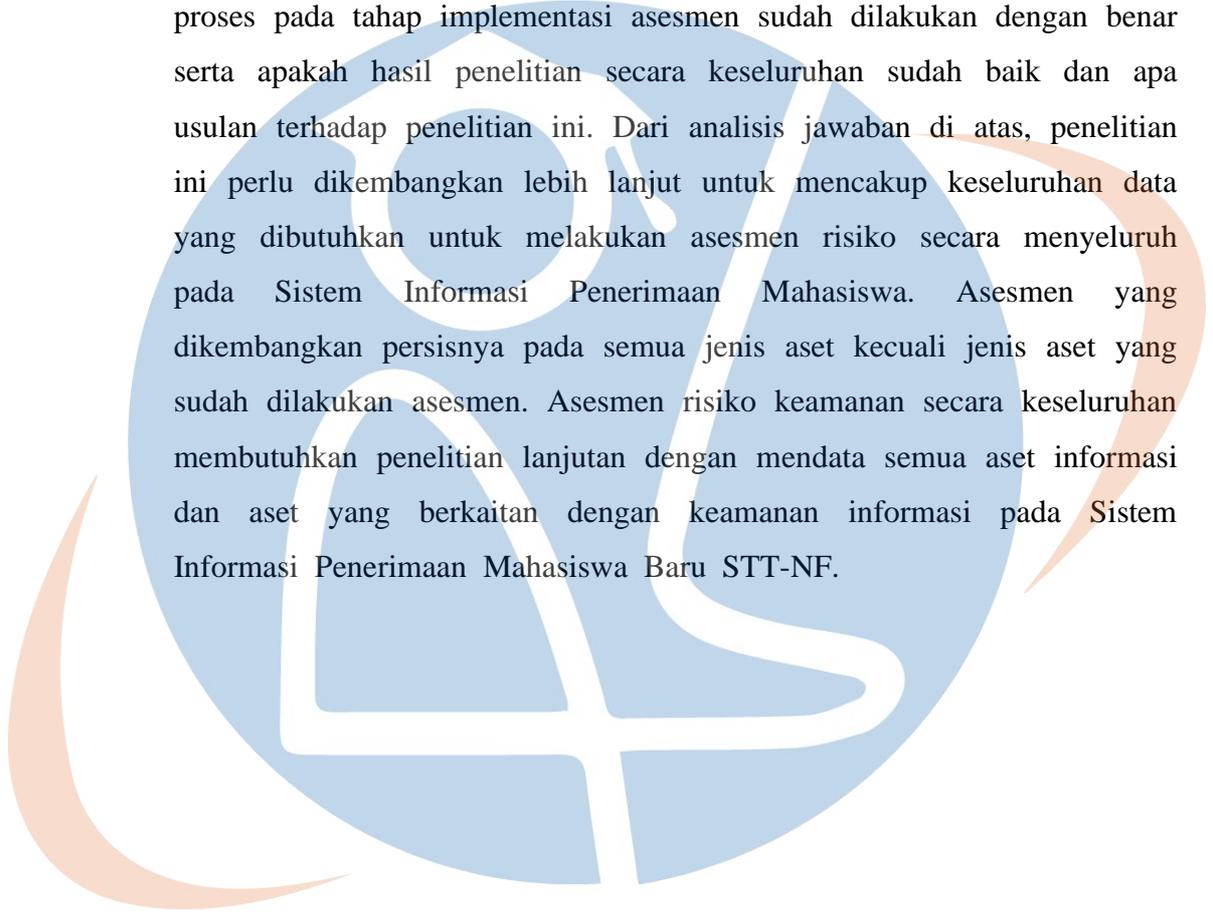
Berikut daftar pertanyaan yang diajukan yang pertama apakah identifikasi risiko pada Sistem Informasi Penerimaan mahasiswa sudah dilakukan dengan benar, yang kedua apakah analisis risiko pada Sistem Informasi Penerimaan Mahasiswa sudah dilakukan dengan benar, yang ketiga apakah daftar penanganan risiko pada tahap evaluasi risiko Sistem Informasi Penerimaan Mahasiswa sudah dilakukan dengan benar, yang keempat apakah hasil penelitian secara keseluruhan sudah baik dan apa usulan terhadap penelitian ini. Hasil analisis dari pertanyaan yang telah diajukan sudah sesuai dengan kuesioner dan rencana penelitian ini

Berikut jawaban setelah daftar pertanyaan telah diajukan untuk pertanyaan kesatu responden pertama memberi jawaban belum sepenuhnya hal ini disebabkan karena risiko yang diketahui pada setiap aset masih sedikit, responden kedua memberi jawaban masih belum lengkap hal ini disebabkan karena belum semua risiko pada setiap aset diketahui, pertanyaan kedua responden pertama memberi jawaban belum sepenuhnya hal ini disebabkan ada kemungkinan analisis risiko yang dilakukan belum tepat, responden kedua memberi jawaban masih belum lengkap hal ini disebabkan analisis risiko belum dilakukan secara keseluruhan.

Pertanyaan ketiga responden pertama memberi jawaban belum sepenuhnya hal ini disebabkan ada kemungkinan hasil analisis risiko belum tepat sehingga daftar penanganan risiko yang dibuat kurang tepat, responden kedua memberi jawaban masih belum lengkap hal ini disebabkan asesmen risiko yang dilakukan hanya di aset teknologi. Pertanyaan keempat responden pertama memberi jawaban pertanyaan

dan jawaban yang perlu dibuat lebih tajam dan fokus terhadap jawaban yang diinginkan hal ini disebabkan saat wawancara jawaban yang diterima oleh penulis tidak sesuai dengan yang diharapkan. Responden kedua memberi jawaban belum baik hal ini disebabkan data yang diperoleh pada hasil penelitian ini belum cukup.

Rangkuman empat pertanyaan berisi pertanyaan apakah semua proses pada tahap implementasi asesmen sudah dilakukan dengan benar serta apakah hasil penelitian secara keseluruhan sudah baik dan apa usulan terhadap penelitian ini. Dari analisis jawaban di atas, penelitian ini perlu dikembangkan lebih lanjut untuk mencakup keseluruhan data yang dibutuhkan untuk melakukan asesmen risiko secara menyeluruh pada Sistem Informasi Penerimaan Mahasiswa. Asesmen yang dikembangkan persisnya pada semua jenis aset kecuali jenis aset yang sudah dilakukan asesmen. Asesmen risiko keamanan secara keseluruhan membutuhkan penelitian lanjutan dengan mendata semua aset informasi dan aset yang berkaitan dengan keamanan informasi pada Sistem Informasi Penerimaan Mahasiswa Baru STT-NF.



STT - NF

## Bab V

### Kesimpulan dan Saran

#### 5.1 Kesimpulan

Dari hasil implementasi dan evaluasi pada bab IV dapat disimpulkan sebagai berikut:

1. Daftar aset informasi pada Sistem Informasi Penerimaan Mahasiswa STT-NF dilakukan dengan menyusun aset Sistem Informasi Penerimaan Mahasiswa sesuai dengan SNI ISO 27005. Cara menyusun aset dilakukan dengan menulis aset yang akan disusun, Kemudian melihat klasifikasi yang tersedia pada Lampiran a dokumen SNI ISO 27005 , kemudian sesuaikan klasifikasi Lampiran a yang sesuai dengan aset. Setelah itu klasifikasi aset dengan klasifikasi yang tersedia di Lampiran a SNI ISO 27005. Ulangi cara tersebut sampai semua aset tersusun dengan benar. Daftar aset informasi pada Sistem Informasi Penerimaan Mahasiswa STT-NF telah berhasil disusun dengan catatan aset sudah disusun dengan baik. Daftar aset yang sudah disusun di antaranya *cloud base, spreadsheet, pengelola informasi PMB*. Untuk daftar aset lainnya dapat dilihat pada tabel identifikasi aset.
2. Asesmen risiko keamanan informasi pada Sistem Informasi Penerimaan Mahasiswa STT-NF dilakukan melalui 3 proses yaitu identifikasi risiko, analisis risiko, evaluasi risiko. Identifikasi risiko dilakukan dengan menuliskan kelemahan aset lalu tuliskan ancaman apa saja yang pernah terjadi baik dari luar maupun dari dalam organisasi kemudian tuliskan dampak dari ancaman yang pernah terjadi setelah itu beri nilai kemungkinan terjadi ancaman sesudah itu beri nilai dampak jika terjadi gangguan. Ulangi proses identifikasi risiko hingga risiko pada semua aset berhasil di identifikasi. Analisis risiko dilakukan dengan mengulangi proses identifikasi risiko kemudian tambahkan isi nilai risiko dalam angka dengan kalikan nilai dampak terjadi gangguan dengan nilai kemungkinan setelah itu

lihat kategori nilai risiko lalu sesuaikan nilai risiko dalam angka dengan kategori nilai risiko kemudian tuliskan nilai risiko dalam angka. Ulangi proses analisis risiko hingga risiko pada aset berhasil dianalisis. Evaluasi risiko dilakukan sendiri oleh penulis dengan cara cek asesmen risiko sudah sesuai dengan teori dan rencana atau belum kemudian memberi rekomendasi aset yang diprioritaskan untuk ditangani kepada perusahaan. Aset yang diberi rekomendasi adalah aset yang memiliki nilai risiko tinggi dan sangat tinggi. Asesmen risiko telah dilakukan dengan catatan asesmen dilakukan hanya pada aset teknologi. Inti dari hasil asesmen risiko adalah asesmen risiko yang dilakukan belum sepenuhnya benar dan belum lengkap.

3. Evaluasi hasil asesmen risiko dilakukan dengan cara memberikan kuesioner kepada bagian penerimaan mahasiswa dan LTSI bagian sistem informasi. Evaluasi hasil asesmen risiko pada Sistem Informasi Penerimaan Mahasiswa STT-NF telah dilakukan. Hasil evaluasi asesmen risiko asesmen sudah dilakukan sesuai dengan panduan yang tertera di dokumen SNI ISO 27005. Dari hasil evaluasi menunjukkan perlu penelitian lebih lanjut yang mencakup keseluruhan aset informasi dan aset lain yang berkaitan dengan keamanan informasi pada Sistem Informasi Penerimaan Mahasiswa Baru STT-NF.

## **5.2 Saran**

Dari hasil evaluasi menunjukkan perlu penelitian lebih lanjut yang mencakup keseluruhan aset informasi dan aset lain yang berkaitan dengan keamanan informasi pada Sistem Informasi Penerimaan Mahasiswa Baru STT-NF. Asesmen risiko yang dilakukan belum sepenuhnya benar dan belum lengkap karena asesmen yang dilakukan hanya pada aset dengan klasifikasi teknologi. Asesmen perlu dilakukan pada semua jenis klasifikasi aset untuk mengetahui apakah sudah dilakukan sepenuhnya dengan benar.

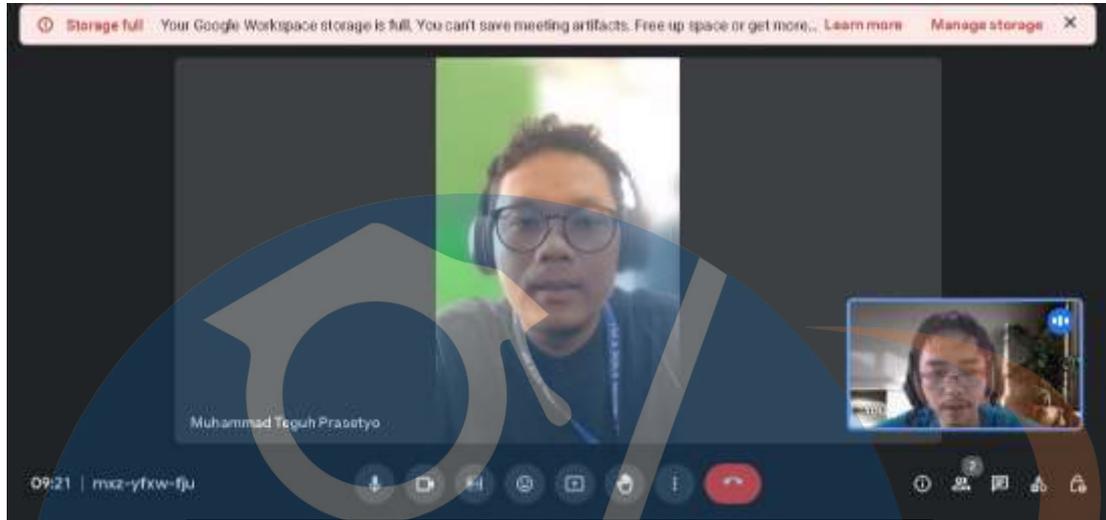
## Daftar Referensi

- [1] F. A. Burhan, "Data Pribadi Nasabah BSI (BRIS) Diduga Bocor, OJK Turun Tangan!," *Bisnis.com*. Diakses: 18 Desember 2023. [Daring]. Tersedia pada:  
<https://finansial.bisnis.com/read/20230516/90/1656624/data-pribadi-nasabah-bsi-bris-diduga-bocor-ojk-turun-tangan>
- [2] K. Teknis 35-04, *SNI ISO/IEC 27001:2022 (Ditetapkan oleh BSN tahun 2023)*. Jakarta: Badan Standardisasi Nasional, 2023. [Daring]. Tersedia pada: [www.bsn.go.id](http://www.bsn.go.id)
- [3] Sekolah Tinggi Teknologi Terpadu Nurul Fikri, "Profil STT Terpadu Nurul Fikri," Nurul Fikri. Diakses: 21 Juni 2022. [Daring]. Tersedia pada:  
<https://nurulfikri.ac.id/profil-sttnf/>
- [4] S. T. Nurul Fikri, "Penerimaan Mahasiswa Baru Sekolah Tinggi Teknologi Terpadu Nurul Fikri," Sekolah Tinggi Teknologi Terpadu Nurul Fikri. Diakses: 17 Januari 2024. [Daring]. Tersedia pada:  
<https://nurulfikri.ac.id/penerimaan-mahasiswa-baru-pmb/>
- [5] F. Mauladani, "Studi Kasus Direktorat Pengembangan Teknologi Dan Sistem Informasi Institut Teknologi Sepuluh Nopember," Institut Teknologi Sepuluh November, Surabaya, 2017.
- [6] N. F. Octariza, "Analisis Sistem Manajemen Keamanan Informasi Menggunakan Standar ISO/IEC 27001 Dan ISO/IEC 27002 Pada Kantor Pusat Jasa Marga," Jakarta, Feb 2019.
- [7] K. Teknis 35-04, *SNI ISO/IEC 27005:2022 (Ditetapkan oleh BSN tahun 2023)*. Jakarta: Badan Standardisasi Nasional, 2023. [Daring]. Tersedia pada: [www.bsn.go.id](http://www.bsn.go.id)
- [8] S. Priadana dan D. Sunarsi, *Metode Penelitian Kuantitatif*, 1 ed. Tangerang Selatan: Pascal Books, 2021.
- [9] W. Annisah, "Implementasi Sistem Informasi Pemasaran Berbasis Web Dalam Kegiatan Jasa Titip Barang Ekspor Impor Pada Bisnis Tourgether.In," Depok, Jun 2022.

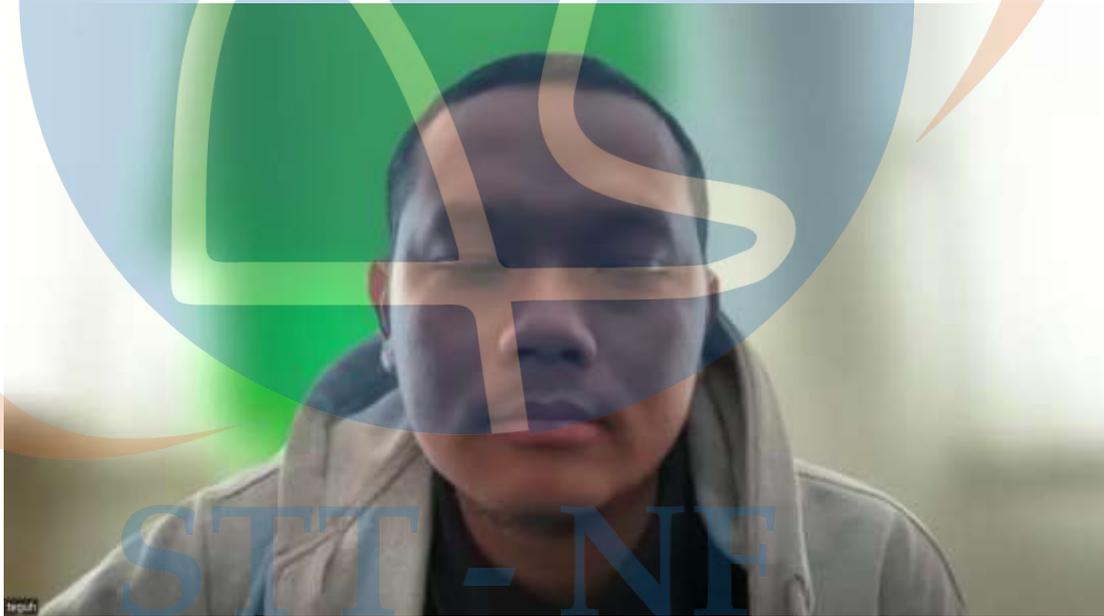
- [10] M. A. Syauqi, “Implementasi Sistem Informasi Reseller Berbasis Web Dengan Cms Wordpress Pada PT Luxima Metro Media,” Jakarta, Mei 2023.
- [11] K. Teknis 35-04, *SNI ISO/IEC 27002:2022 (Ditetapkan oleh BSN tahun 2022)*. Jakarta, 2022. [Daring]. Tersedia pada: [www.bsn.go.id](http://www.bsn.go.id)



## Lampiran



Gambar 3 Wawancara mengenai Sistem Informasi Penerimaan Mahasiswa



Gambar 2 Wawancara aset Sistem Informasi Penerimaan Mahasiswa

## Kuesioner Evaluasi Hasil Asesmen Risiko (Evaluasi TA)

Jawaban ini tidak akan disebarluaskan dan hanya digunakan untuk penulisan tugas akhir.

Email responden ([teguh.kun@gmail.com](mailto:teguh.kun@gmail.com)) dicatat saat formulir ini dikirimkan.

Apakah identifikasi risiko pada Sistem Informasi Penerimaan Mahasiswa sudah dilakukan dengan benar ?

Belum sepenuhnya

Apakah analisis risiko pada Sistem Informasi Penerimaan Mahasiswa sudah dilakukan dengan benar? \*

Belum sepenuhnya

Apakah daftar penanganan risiko pada tahap evaluasi risiko Sistem Informasi Penerimaan Mahasiswa sudah dibuat dengan benar? \*

Belum sepenuhnya

Apakah hasil penelitian secara keseluruhan sudah baik ? Apa usulan perbaikan terhadap penelitian ini? \*

Pertanyaan dan jawaban yang perlu dibuat lebih tajam dan fokus terhadap jawaban yang diinginkan

Konten ini tidak dibuat atau didukung oleh Google

Google Formulir

Gambar 4 Jawaban Responden Kuesioner

# STT - NF

## Kuesioner Evaluasi Hasil Asesmen Risiko (Evaluasi TA)

Jawaban ini tidak akan disebarluaskan dan hanya digunakan untuk penulisan tugas akhir

Email responden ([edo@nurulfikri.ac.id](mailto:edo@nurulfikri.ac.id)) dicatat saat formulir ini dikirimkan.

Apakah identifikasi risiko pada Sistem Informasi Penerimaan Mahasiswa sudah dilakukan dengan benar ?

Masih belum lengkap

Apakah analisis risiko pada Sistem Informasi Penerimaan Mahasiswa sudah dilakukan dengan benar? \*

Masih belum lengkap

Apakah daftar penugasan risiko pada tahap evaluasi risiko Sistem Informasi Penerimaan Mahasiswa sudah dibuat dengan benar ? \*

Masih belum lengkap

Apakah hasil penelitian secara keseluruhan sudah baik ? Apa usulan perbaikan terhadap penelitian ini ? \*

Belum baik

Konten ini tidak dibuat atau didukung oleh Google.

Google Formulir

Gambar 5 Jawaban Responden Kuesioner

# STT - NF