SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

ANALISIS PENERAPAN SISTEM MANAJEMEN KEAMANAN INFORMASI PADA WEBSITE OFFICIAL STT NF DENGAN SNI ISO/IEC 27001:2022

TUGAS AKHIR

EPRI LIYANTO
0110120113

PROGRAM STUDI SISTEM INFORMASI
DEPOK
AGUSTUS 2024

SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

ANALISIS PENERAPAN SISTEM MANAJEMEN KEAMANAN INFORMASI PADA WEBSITE OFFICIAL STT NF DENGAN SNI ISO/IEC 27001:2022

TUGAS AKHIR

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer

EPRI LIYANTO

0110120113

PROGRAM STUDI SISTEM INFORMASI

DEPOK

AGUSTUS 2024

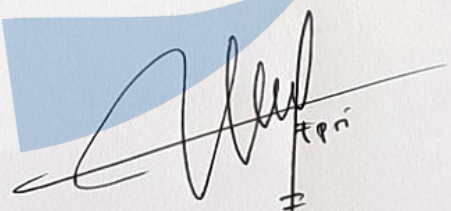
HALAMAN PERNYATAAN ORISINALITAS

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

Nama : Epri Liyanto

NIM : 0110120113

Depok, 6 Agustus 2024



Epri Liyanto

HALAMAN PENGESAHAN

Tugas Akhir ini diajukan oleh :

Nama	: Epri Liyanto
NIM	: 0110120113
Program Studi	: Sistem Informasi
Judul Tugas Akhir	: Analisis Penerapan Sistem Manajemen Keamanan Informasi pada Website Official 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 Komputer pada Program Studi Sistem Informasi Sekolah Tinggi Teknologi Terpadu Nurul Fikri

DEWAN PENGUJI

Pembimbing	**Penguji**
Drs. Rusmanto, M.M.	Dr. Amalia Rahmah, S.T., M.T.

Ditetapkan di : Depok

Tanggal : 6 Agustus 2024

KATA PENGANTAR

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

1. Allah SWT atas berkat dan rahmat-Nya untuk menyelesaikan Tugas Akhir ini.
2. Orang tua dan semua anggota keluarga yang telah memberikan dorongan baik secara moril maupun materil dalam penyelesaian tugas ini.
3. Bapak Dr. Lukman Rosyidi, S.T., M.M., M.T. selaku Ketua Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
4. Ibu Misna Azqia, M.Kom. selaku Ketua Program Studi Sistem Informasi Sekolah Tinggi Teknologi Terpadu Nurul Fikri, pembimbing akademik, dan dosen penguji yang telah memberikan saran dan masukan untuk penelitian ini.
5. Ibu Dr. Amalia Rahmah, S.T., M.T. selaku pembimbing akademik dan dosen penguji yang telah membimbing selama empat tahun perkuliahan sampai dengan dapat menyelesaikan perkuliahan.
6. Bapak Drs. Rusmanto, M.M. selaku Dosen Pembimbing Tugas Akhir penulis dalam menyelesaikan penulisan ilmiah ini.
7. Para dosen di lingkungan Sekolah Tinggi Teknologi Terpadu Nurul Fikri yang telah membimbing penulis dalam menuntut ilmu yang telah diberikan.
8. Teman-teman seperjuangan angkatan 2020 khususnya Sistem Informasi 2020 dan teman sahabat yang paling dekat yaitu Muhammad Adli Azzam yang telah membersamai selama 4 tahun berjuang menuntut ilmu bersama hingga akhir.

Dalam penulisan ilmiah ini tentu saja masih banyak terdapat kekurangan yang mungkin disebabkan oleh keterbatasan kemampuan dan pengetahuan yang penulis miliki. Dengan demikian penulis telah berusaha menyelesaikan penulisan ilmiah ini sebaik mungkin. Oleh karena itu, apabila terdapat kekurangan di dalam penulisan ilmiah ini, dengan rendah hati penulis menerima kritik dan saran dari pembaca.

Akhir kata, penulis berharap Allah SWT berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga skripsi ini membawa manfaat bagi pengembangan ilmu.

Depok, 6 Agustus 2024

Penulis

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 : Epri Liyanto

NIM : 0110120113

Program Studi : Sistem Informasi

Jenis karya : Tugas Akhir

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:

"Analisis Penerapan Sistem Manajemen Keamanan Informasi pada Website Official 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 : 6 Agustus 2024

Yang Menyatakan

Epri Liyanto

ABSTRAK

Nama : Epri Liyanto
NIM : 0110120113
Program Studi : Sistem Informasi
Judul : Analisis Penerapan Sistem Manajemen Keamanan Informasi pada Website Official STT NF dengan SNI ISO/IEC 27001:2022

Website Official STT NF perlu dijaga keamanannya dengan penerapan Sistem Manajemen Keamanan Informasi berbasis standar nasional dan internasional SNI ISO/IEC 27001:2022. Adapun tujuan penelitian ini yaitu untuk mengimplementasikan serta mengevaluasi Sistem Manajemen Keamanan Informasi (SMKI) pada website official STT NF dengan batasan hanya sampai tahapan asesmen risiko. Metode yang digunakan dalam penelitian ini yaitu kualitatif atau wawancara dengan pengelola *website* tersebut untuk kebutuhan analisis maupun evaluasi hasil. Asesmen risiko yang dilakukan dengan tahapan menentukan kriteria risiko, menentukan level risiko, keberterimaan risiko, dan terakhir evaluasi risiko. Hasil dari penelitian diketahui bahwa *website official* STT NF belum menerapkan standar keamanan nasional, sehingga selama beroperasi pernah mengalami peretasan yaitu serangan *malware* yang mengakibatkan sistem informasi tersebut tidak dapat diakses dan terjadi *error* ketika digunakan oleh pengguna atau lembaga lain. Hasil asesmen risiko dinilai tinggi karena keretasan tersebut kemungkinan dapat terjadi satu kali dalam setahun atau kurang dari dua tahun dan menimbulkan dampak yang merugikan karena sistem informasi tidak dapat berjalan selama lima hari. Maka dari itu dapat disimpulkan bahwa penerapan standar keamanan nasional perlu diterapkan sehingga sistem informasi dapat terhindar dari keretasan maupun ancaman yang sewaktu-waktu dapat terjadi walaupun sistem informasi tersebut menggunakan keamanan dari *provider*.

Kata kunci: Sistem informasi, SMKI, asesmen risiko

ABSTRACT

Name : Epri Liyanto

NIM : 0110120113

Study Program : Information System

Title : Analysis of Application of Information Security Management Systems on the Official Website STT NF with SNI ISO/IEC 27001:2022

The official website of STT NF needs to be safeguarded by the implementation of an Information Security Management System based on national and international standards SNI ISO/IEC 27001:2022. The purpose of this research is to implement and evaluate the Information Security Management System (ISMS) on the official website of STT NF with restrictions only to the risk assessment stage. The methods used in this research are qualitative or interviews with the website administrator for analysis or evaluation of results. Risk assessment performed by phases determines risk criteria, determines the level of risk, accepts risk, and finally risk assessment. As a result of the research, it is known that the official website of STT NF has not implemented national security standards, so during its operation it has suffered a malware attack that causes the information system to be inaccessible and errors occur when used by users or other institutions. The risk assessment results are highly valued because the framework is likely to occur once a year or less than two years and has a negative impact because the information systems can not run for five days.

Keywords: *Information systems, SMKI, risk assessment*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan informasi menjadi salah satu hal yang penting karena sebuah sistem informasi tanpa adanya keamanan untuk melindungi data dan aset informasi maka sistem tersebut akan terancam kerahasiaannya. Hal ini tentu dapat menimbulkan kerugian bagi suatu organisasi ataupun perusahaan. Keamanan data dan aset informasi juga dapat berpengaruh terhadap kelancaran bisnis, sehingga dengan adanya sistem manajemen keamanan informasi kelancaran bisnis dan data aset informasi pun akan terjaga dan aman dari segalan ancaman.

Penerapan asesmen risiko tentu merupakan tahapan dalam pengamanan aset dan data informasi suatu perusahaan atau organisasi. Setiap perusahaan atau organisasi pasti mempunyai kerahasiaan data dalam sistem yang harus dilindungi. Kelengkapan dokumen kebijakan sistem informasi harus sesuai dengan standar nasional/internasional seperti SNI ISO/IEC 27001:2022, yang mana di dalamnya terdapat panduan dan aturan dalam penerapan keamanan informasi. SNI ISO/IEC 27001:2022 dengan judul Keamanan Informasi, Keamanan *Cyber* dan Proteksi privasi - Sistem Manajemen Keamanan Informasi – Persyaratan, ISO/IEC 27001:2022 merupakan revisi dari SNI ISO/IEC 27001:2013, Teknologi Informasi - Teknik Keamanan – Sistem Manajemen Keamanan Informasi – Persyaratan.

Dari penjelasan yang disebutkan di atas, *Website Official* STT NF yang merupakan salah satu situs web kampus yang harus dijaga dengan penerapan Sistem Manajemen Keamanan Informasi yang mengacu pada dokumen standar nasional/internasional yaitu SNI ISO/IEC 27001:2022 agar *Website Official* STT NF dapat terjaga keamanannya dengan pengimplementasian dan evaluasi hasil implementasi Sistem Manajemen Keamanan Informasi tersebut. Mengapa perlu dijaga? Karena dalam *website official* STT NF pernah terjadi serangan *malware* yang mana hal ini mengganggu operasional *website*

tersebut, sehingga dapat terjadi sabotase data yang digunakan tidak sebagaimana mestinya.

Salah satu penelitian yang menjadi contoh kasus yaitu pada penelitian oleh Athallariq dan Nilo (2022) yang berjudul Penilaian Risiko pada Perusahaan dengan Berfokus pada Area Keamanan Informasi Menggunakan Iso 27001:2022. Dalam penelitian tersebut dipaparkan bahwa Semua informasi digital rentan terhadap serangan *cyber*, yang dibuktikan dengan survei proyek *honeynet* dari BSSN yang menyatakan 9,6% serangan *cyber* meningkat lebih banyak pada tahun 2021 dibanding dengan tahun 2020. Jenis serangan *cyber* yang sering terjadi yaitu *Ransomware* dan pelanggaran data. Oleh karena itu, Perseroan perlu memperhatikan risiko terkait SMKI. Standar ISO/IEC 27001 sering digunakan untuk mengidentifikasi apakah keamanan sistem informasi harus diterapkan. Untuk membuat Sistem Manajemen Keamanan Informasi (SMKI), perlu mematuhi persyaratan yang diuraikan dalam ISO/IEC 27001:2022. Dalam kasus ini menjadi salah satu acuan untuk implementasi SMKI pada website official STT NF agar terjaga dari serangan ataupun ancaman *cyber* dan pelanggaran data.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan pada bagian sebelumnya, rumusan masalah yang dapat disimpulkan sebagai berikut:

1. Bagaimana mengimplementasikan Sistem Manajemen Keamanan Informasi dengan SNI ISO/IEC 27001:2022 pada Sistem *Website Official* STT-NF?
2. Bagaimana mengevaluasi hasil implementasi Sistem Manajemen Keamanan Informasi dengan SNI ISO/IEC 27001:2022 pada Sistem *Website Official* STT-NF?

1.3 Tujuan dan Manfaat Penelitian

Tujuan dari penelitian ini:

1. Menjelaskan proses implementasi Sistem Manajemen Keamanan Informasi dengan SNI ISO/IEC 27001:2022 pada Sistem *Website Official* STT-NF.

2. Menjelaskan proses evaluasi hasil implementasi Sistem Manajemen Keamanan Informasi dengan SNI ISO/IEC 27001:2022 pada Sistem *Website Official* STT-NF untuk digunakan sebagai tolak ukur apakah *website official* STT NF tersebut sudah dalam standar nasional atau belum.

Manfaat dari penelitian ini:

1. Bagi peneliti
    a. Menambah wawasan dalam penelitian keamanan informasi agar suatu *website* tersebut sesuai standar dan aman dari ancaman.
    b. Mengetahui apa saja yang harus dilakukan agar keamanan informasi suatu perusahaan atau organisasi sudah standar nasional.
2. Bagi Kampus
    a. Sebagai bahan untuk menambah referensi yang ditujukan untuk keamanan sistem informasi kampus.
    b. Sebagai acuan untuk menstandarkan keamanan informasi yang selama ini belum diterapkan.

1.4 Batasan Masalah

Dalam penulisan tugas akhir ini memberikan batasan masalah yang mana pengimplementasian SMKI dengan SNI ISO/IEC 27001:2022 ini dibatasi sampai proses asesmen risiko keamanan informasi. Tugas akhir ini tidak melaksanakan hingga penanganan risiko dan pelaksanaan kontrol keamanan.

1.5 Sistematika Penulisan

1. BAB I PENDAHULUAN, dalam bab ini yaitu bab awal yang memberikan gambaran dasar mengenai bagaimana cara penelitian ini berjalan untuk menganalisa penerapan SNI ISO/IEC 27001:2022. Isi dari bab ini yaitu bahasan tentang latar belakang, rumusan masalah, tujuan dan manfaat penelitian, batasan masalah, dan sistematika penulisan.
2. BAB II KAJIAN LITERATUR, dalam bab ini yaitu berisi kajian mengenai teori pendukung dari penelitian analisis penerapan Sistem manajemen Keamanan Informasi (SMKI) yang dilakukan serta tabel perbandingan

dengan peneliian yang sudah ada sebelumnya dengan menggunakan tema yang sama terutama dalam penerapan SNI ISO/IEC 27001:2022.

3. BAB III METODOLOGI PENELITIAN, bab ini membahas langkah-langkah dalam melakukan penelitian, yang mana dimulai dari yang sudah dilakukan hingga yang akan dilakukan.
4. BAB IV HASIL PENELITIAN DAN PEMBAHASAN, dalam bab ini yaitu isi dari penelitian yang membahas hasil dari penelitian, yaitu dengan melakukan implementasi dan evaluasi hasil dari implementasi tersebut.
5. BAB V KESIMPULAN DAN SARAN, pada bab ini berisi kesimpulan dan saran yang menjawab tujuan serta rumusan masalah dari penelitian ini. Hingga didapatkan hasil yang dapat memberikan solusi terhadap kekurangan yang ada.

BAB II
KAJIAN LITERATUR

2.1 Landasan Teori

2.1.1 Sistem Manajemen Keamanan Informasi

Sebuah sistem informasi pastinya harus dilindungi keamanannya, agar data-data yang ada aman dari segala macam ancaman, maka dari itu standar sistem keamanan informasi harus diterapkan untuk mencegah kemungkinan buruk yang terjadi. Pemahaman dan penerapan yang baik terhadap Sistem Manajemen Keamanan Informasi (SMKI) akan sangat berpengaruh untuk keamanan data-data yang ada di dalam sistem informasi.

Keamanan informasi merupakan melindungi serta mengamankan aset informasi dari ancaman yang dapat membahayakan. Dapat juga didefinisikan sebagai perlindungan aset informasi dari berbagai macam ancaman yang mungkin dapat terjadi sebagai upaya untuk memastikan atau menjamin kelangsungan bisnis, meminimalkan risiko bisnis, dan memaksimalkan atau mempercepat pengambilan investasi dan peluang bisnis. [1]

Keamanan informasi sangat penting diterapkan dan diperhatikan dengan baik. Karena dengan menerapkan keamanan informasi semua data-data kerahasiaan dan aset informasi yang dimiliki sebuah perusahaan/organisasi akan terjaga dan terlindungi dengan baik dari segala ancaman dan sabotase data yang bisa terjadi. Keamanan informasi dimaksudkan untuk memastikan keberlangsungan suatu organisasi atau bisnis yang memilikinya. Menjaga keamanan informasi akan membantu meminimalkan risiko dan memaksimalkan pertumbuhan bisnis. [2]

Sistem Manajemen Keamanan Informasi merupakan sebuah metode atau cara untuk meningkatkan keamanan data dengan memanfaatkan pendekatan risiko untuk melindungi dan mengelola informasi. Lebih lengkapnya Setyaningsih (2022) menyatakan “Sistem Manajemen Keamanan Informasi (SMKI) adalah pendekatan sistematis untuk mengelola informasi perusahaan yang sensitif agar tetap aman. SMKI mencakup orang, proses dan sistem teknologi informasi yang menerapkan

manajemen risiko. ISO 27001: 2013 berfokus tidak hanya pada aspek teknologi informasi saja, melainkan juga aset bisnis penting,sumber daya dan proses dalam organisasi. Standar ini terdiri dari 10 klausul dan lampiran *annex*, yang secara sistematis membentuk sebuah gambaran utuh dari siklus *Plan- Do-Check-Act* (PDCA *Cycle*)." [3]

Dengan penerapan Sistem Manajemen Keamanan Informasi (SMKI) ini tentunya semua aset informasi dan data-data rahasia perusahaan/organisasi dapat terlindungi dari ancaman yang mungkin terjadi. Menurut Rhenn (2023) "Agar dapat tercapai keamanan informasi, diperlukan berbagai macam upaya teknis serta didukung dari berbagai kebijakan dan prosedur manajemen yang telah sesuai dengan kebutuhan dan peruntukannya. Maka dari itu, diperlukan sebuah sistem untuk mengatur keamanan informasi. Sitem itu disebut dengan Sistem Manajemen Keamanan Informasi (SMKI) atau dalam bahasa Inggris dikenal dengan *Information Security Management System* (ISMS). [2]

Sistem Manajemen Keamanan Informasi (SMKI) terdiri dari sejumlah komponen yang saling terkait yang digunakan untuk mengelola dan melindungi keamanan informasi yang dimiliki oleh suatu organisasi atau perusahaan. Komponen kerahasiaan (*confidentiality*) melindungi data atau informasi, memastikan bahwa hanya orang yang berwenang yang dapat mengaksesnya, dan integritas (*integrity*) melindungi data yang dikirim, diterima, dan disimpan. Juga ketersediaan (*avaibility*) informasi, elemen yang memastikan bahwa data dapat diakses saat dibutuhkan dan memastikan bahwa orang yang berhak dapat menggunakan informasi dan perangkat yang terkait, jika diperlukan. [1]

2.1.2 SNI ISO/IEC 27001:2022

Salah satu standar Sistem Manajemen Keamanan Informasi adalah SNI/ISO 27001 yang merupakan salah satu seri ISO yang menitikberatkan pada pengembangan program keamanan, termasuk juga di dalamnya konteks organisasi, kepemimpinan, perencanaan, *support*, dokumentasi, operasi, penilaian kerja, dan peningkatan berkelanjutan. ISO 27001 biasanya digunakan untuk meningkatkan reputasi, meningkatkan nilai persaingan, dan mendukung program keamanan data pemerintah atau pihak ketiga. Secara khusus, ISO 27001 diperlukan oleh organisasi

atau perusahaan untuk melindungi aset dan privasi informasi yang dimiliki agar aman.

ISO 27001 telah diatur dalam peraturan Menteri Komunikasi dan Informatika (Permenkominfo) nomor 4 tahun 2016 tentang Sistem Menejemen Pengamanan Informasi. Dalam pasal 7 Permen tersebut mengatur bahwa bagi penyelenggara sistem elektronik strategis harus menerapkan standar SNI ISO/IEC 27001 terutama bagi penyelenggara sistem elektronik tinggi. Maka dari itu dapat disimpulkan bahwa ISO 27001 telah diakui urgensinya dalam mengamankan informasi data di Indonesia.

ISO/IEC 27001:2022 adalah versi terbaru dari standar Sistem Manajemen Keamanan Informasi (SMKI), yang memberikan pedoman bagi organisasi untuk menetapkan, menerapkan, memelihara, dan meningkatkan sistem manajemen keamanan informasi mereka. Standar ini dirancang agar dapat diterapkan pada semua jenis, ukuran, dan sifat organisasi, dan didasarkan pada pendekatan manajemen risiko. ISO/IEC 27001:2022 menetapkan persyaratan SMKI untuk mencapai sertifikasi, menguraikan tujuh elemen utama: penetapan, implementasi, pengoperasian, pemantauan, peninjauan, pemeliharaan, dan peningkatan sistem. Panduan ini dimaksudkan untuk digunakan bersama dengan ISO/IEC 27002, yang memberikan pedoman rinci mengenai kontrol keamanan informasi.

ISO/IEC 27001:2022 diakui karena tingkat legitimasi keluarannya yang tinggi, sehingga memungkinkannya mencapai tujuan secara efektif untuk memastikan kerahasiaan, integritas, dan ketersediaan aset bisnis penting, membangun budaya dan kesadaran keamanan informasi, dan memitigasi risiko kehilangan peluang bisnis. Namun, standar ini mungkin perlu dilengkapi dengan sertifikasi tambahan atau mencari dukungan dari standar lain untuk mengatasi tantangan tertentu, seperti meningkatkan kesadaran keamanan informasi dalam organisasi.[1]

[1] [6]

2.1.3 Asesmen Risiko SNI ISO/IEC 27001:2022

Ancaman risiko yang dapat menyebabkan retasnya keamanan dalam sebuah sistem informasi baik dalam perusahaan maupun pendidikan. Maka dari itu diperlukan adanya asesmen risiko yang mencangkup Sistem Manajemen Keamanan Informasi (SMKI) untuk menghindari berbagai macam ancaman. Sistem Manajemen Keamanan Informasi (SMKI) yang merupakan suatu bentuk tahapan yang dibuat berdasarkan pendekatan risiko bisnis dengan tahapan perencanaan (*plan),* Mengimplementasikan dan mengoperasikan *(do),* Memonitoring dan meninjau *(check),* serta memelihara dan juga mengembangkan *(act).* Dalam hal ini tentu dapat mendukung sistem informasi yang aman dari segala macam ancaman. Melakukan asesmen risiko salah satu bentuk untuk mencegah terjadinya hal-hal yang dapat merusak atau meretas sistem tersebut.

Asesmen risiko merupakan salah satu kegiatan yang mana dalam tahap ini merupakan proses awal untuk menerapkan standar keamanan informasi. Dalam tahap asesmen risiko ini, dilakukan untuk menganalisa kerentanan atau ancaman apa saja yang terjadi pada sebuah sistem informasi yang ddapat menjadi bahan evaluasi untuk penerapan Sistem Manajemen Keamanan Informasi.

Landasan yang paling awal untuk keberlanjutan keamana informasi yaitu *CIA Triad* yang merupakan kerangka kerja yang digunakan untuk keamanan informasi. Ada tiga aspek yang utama diantaranya yaitu *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Avaibility* (ketersediaan). Tiga aspek ini tentu sangat penting dalam pengelolaan keamanan sistem informasi yang mana dengan tiga aspek ini dapat membantu perusahaan untuk membangun sistem keamanan yang tidak mudah terjadi kerentanan ataupun ancaman.

ISO 27001 atau standar keamanan informasi dengan *CIA Triad* ini tentu saling berhubungan dalam membangun sistem keamanan informasi yang mana ISO 27001 dapat membantu organisasi atau perusahaan untuk menerapkan konsep *CIA Triad* tersebut. Yang pertaman *Confidentiality* (Ketersediaan) yang memastikan informasi hanya sistem diakses oleh orang yang berkepentingan, dalam hal ini ISO 27001 memerlukan organisasi yang dapat mengidentifikasi hal-hal yang menjadi informasi sensitif dan mengambil langkah-langkah untuk menjaga kerahasiaan data terjaga yang mencangkup pengaturan izin akses dan enskripsi data. Kedua, yaitu

Integrity (Integritas) yang memastikan kelengkapan, keakuratan, dan kebutuhan informasi. ISO 27001 juga memerlukan organisasi yang dapat memastikan terjaganya data agar tidak terjadi perubahan yang tidak sah. Ketiga, *Avaibility* (Ketersediaan), memastikan informasi ada dan tersedia saat informasi tersebut dibutuhkan. ISO 27001 yang juga memerlukan organisasi yang dapat memastikan ketersediaan data dan sistem. [4]

Tahapan-tahapan asesmen risiko dalam SNI ISO/IEC 27001:2022 adalah sebagai berikut :

1. Tahap pertama

Tahap yang pertama yaitu menentukan kriteria nilai kemungkinan dan dampak yang akan terjadi. Nilai kriteria dengan skala tingkatan 1-5.

Nilai kemungkinan :

1. Nilai 1 (sangat rendah/kecil) : kemungkinan terjadi sangat jarang hanya selama 1x selama lebih dari dua tahun.
2. Nilai 2 (rendah/kecil) : kemungkinan terjadi 1x dalam setahun hingga dua tahun
3. Nilai 3 (sedang) : kemungkinan terjadi 2x sampai 6x pertahun
4. Nilai 4 (tinggi) : kemungkinan terjadi 7x hingga 11x pertahun.
5. Nilai 5 (sangat tinggi) : kemungkinan terjadi 12x pertahun atau 1x dalam satu bulan

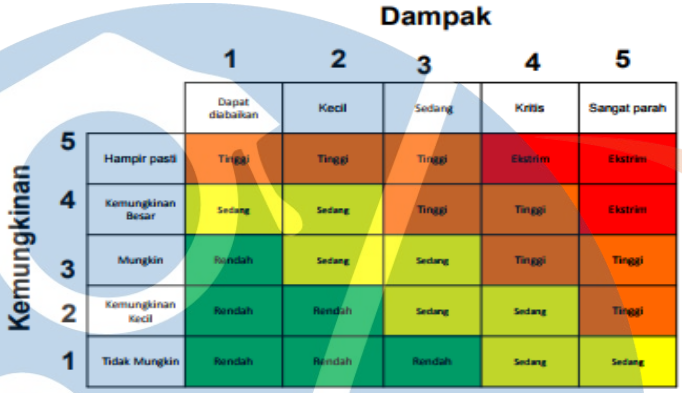
Nilai dampak :

1. Nilai 1 (sangat rendah/kecil) : pekerjaan tertunda selama kurang dari satu jam
2. Nilai 2 (rendah) : pekerjaan tertunda satu jam hingga kurang dari dua jam
3. Nilai 3 (sedang) : pekerjaan tertunda selama dua jam hingga kurang dari tiga jam
4. Nilai 4 (tinggi) : pekerjaan tertunda selama tiga jam hingga kurang dari enam jam
5. Nilai 5 (sangat tinggi) : pekerjaan tertunda selama enam jam atau lebih

2. Tahap kedua

Pada tahap kedua ini yaitu menentukan level risiko yaitu dengan mengalikan nilai kemungkinan dengan nilai dampak kerugian yang terjadi. Dalam tahapan ini dapat diketahui berada dilevel mana kerentanan yang terjadi. tabel dibawah ini menunjukkan kriteria asesmen risiko.

Tabel 1. Kriteria Asesmen Risiko [5]



Sumber : Administrator (2020)

Metode analisis risiko ini dengan kuantitatif atau dengan angka-angka yaitu dengan ketentuan level risiko rendah untuk hasil perkalian satu sampai dengan empat, level risiko sedang untuk hasil perkalian lima sampai dengan sembilan,level risiko tinggi untuk hasil perkalian 10 sampai dengan 12, dan level risiko sangat tinggi atau ekstrim yaitu untuk hasil perkalian lebih dari 12, yaitu 16, 20, dan 25.

3. Tahap ketiga

Dalam tahap ini yaitu menentukan risikonya dapat diterima dan tidak dapat diterima berdasarkan kriteria penerimaan risiko yang ditentukan level risiko yang dilakukan ditahap kedua, hanya level rendah yang dapat diterima risikonya.

Tabel 2. Kategori Level Risiko

Kategori Level Risiko	**Tindakan Yang Diambil**
Rendah	Tidak diperlukan tindakan (*Acceptable*)
Sedang	Disarankan diambil tindakan jika bersedia sumber daya *(Sumpplementary Issue)*
Tinggi	Diperlukan tindakan untuk mengelola risiko *(Issue)*
Sangat Tinggi	Diperlukan tindakan segera untuk mengelola risiko *(Unacceptable)*

4. Tahap keempat

Tahapan terakhir asesmen risiko ini evaluasi risiko dengan dua langkah dibawah ini:

1. Mengecek kembali hasil asesmen risiko, apakah kemungkinan dan dampak sudah sesuai dengan kriteria yang ditentukan, dan penerimaan risiko sudah sesuai atau belum dengan kriteria yang ditentukan.
2. Menentukan prioritas untuk penanganan risiko bagi asset yang level risikonya tidak dapat diterima.

2.1.4 Evaluasi dan Penanganan Risiko

Proses penanganan risiko tentu dapat terlaksana setelah adanya asesmen risiko yang telah dilakukan. Dalam tahap atau proses ini dapat ditentukan untuk penanganan yang dilakukan untuk menyelesaikan atau menguraikan risiko agar dapat ditangani. Dengan solusi yang tepat dan dapat mencegah terjadi kembali juga menghindari ancaman yang sewaktu-waktu dapat menyerang. Pengelolaan risiko dapat dengan cara mengidentifikasi atau mengsistemisasi risiko yang akan timbul. Lalu untuk mengurangi, mencegah, atau juga sistem dikatakan sebagai proses yang berupaya untuk meminimalisir dampak negatif dari risiko yang ada. Kemudian melakukan evaluasi terhadap risiko yang muncul dan bagaimana cara yang tepat untuk menanggulanginya.

Penanganan risiko dengan ISO 27001 melibatkan beberapa langkah penting untuk mengelola risiko keamanan informasi dalam suatu organisasi. Berikut adalah langkah-langkah tersebut:

1. Metodologi Penilaian Risiko
   a. Aturan tentang cara menerapkan manajemen risiko ditentukan
   b. Pengukuran risiko secara kualitatif maupun kuantitatif ditentukan
2. Penilaian Risiko:
   a. Menuliskan daftar aset, kerentanan dan ancaman yang berhubungan dengan aset-aset.
   b. Nilai dampak dan potensi dari kombinasi berbagai ancaman.
   c. Menghitung tingkat risiko.
3. Penanganan Risiko:

a. Fokus pada risiko yang paling penting dan tidak dapat diterima.
b. Ada empat opsi penanganan risiko yang dapat dipilih:
    - Terapkan kontrol keamanan dari Lampiran A ISO 27001.
    - Transfer risiko ke pihak lain.
    - Hindari risiko dengan menghentikan kegiatan yang terlalu berisiko.
    - Menerima risiko jika biaya untuk mengurangi risiko lebih tinggi dibandingkan kerusakan yang ditimbulkan.

4. Pembuatan Laporan Penilaian Risiko:
    a. Mendokumentasikan semua langkah yang telah dilakukan sebelumnya dalam bentuk laporan.
    b. Laporan yang dibuat dapat berguna untuk tim audit dan pemilik atau pemimpin organisasi yang ingin meninjau kembali kejadian di masa lampau.
5. Pembuatan Dokumen Pernyataan Pemberlakuan:
    a. Dokumen akan menunjukkan kondisi keamanan perusahaan secara nyata.
    b. Dokumen ini juga penting untuk membantu tugas tim audit.
6. Penyusunan Rencana Penanganan Risiko:
    a. Menentukan berbagai hal seperti menugaskan tim yang akan mengimplementasikan tindakan serta menentukan waktu dan *budget.*

Dengan mengikuti langkah-langkah di atas, organisasi dapat lebih efektif dalam mengelola risiko keamanan informasi dan meningkatkan keamanan data. [5]

2.2 Sistem Informasi Manajemen Konten STT Terpadu Nurul Fikri

2.2.1 Sistem Informasi

Di era serba digital ini, semua informasi, berita, dan apapun itu dapat diakses melalui internet, media sosial dan berbagai *platform* digital yang marak saat ini. Sistem informasi merupakan transformasi digital yang merambah ke segala bidang, baik itu ekonomi, bisnis, industri, maupun pendidikan. Sistem informasi menjadi salah satu aktor penting dalam sebuah organisasi dalam mengelola dan memenejemen informasi.

Sistem informasi adalah sistem yang menggabungkan pekerjaan manusia dan teknologi untuk membantu kegiatan manajemen dan operasional. Data dan

arsip baru akan tersimpan dan terekam dengan baik, sehingga pengguna dapat dengan mudah menemukan data dan informasi yang dibutuhkan. [4]

Dalam sebuah organisani/perusahan dan pasar elektronik sistem informasi digunakan untuk menjalankan rantai pasokan. Banyak perusahaan besar yang saat ini yang dibangun sistem informasi. Perusahaan memanfaatkan sistem informasi untuk proses keuangan, mengelola sumber daya manusia, menjangkau pelanggan yang potensial dengan promosi online, dan lain sebagainya. Dan ini menjadi potensi yang besar untuk memajukan sebuah organisasi/perusahaan dan pasar elektronik.

Pada dasarnya sistem informasi digunakan untuk kepentingan umum, yang berfokus pada layanan umum untuk berbagai kegunaan. Contohnya, sistem informasi yang digunakan untuk menyebarkan informasi yang mempromosikan atau memperkenalkan produk, layanan, ataupun jasa. Kegunaan sistem informasi juga tergantung pada organisasi/perusahaannya dibidangnya masing-masing.

Dilihat dari kegunaannya sistem informasi dinilai sangat dibutuhkan oleh suatu instansi/perusahaan. Dengan adanya sistem informasi, kinerja dari sebuah perusahaan atau instansi akan lebih sistematis dan terarah. Tetapi agar dapat tercapai dampak yang positif, semua unsur yang ada pada sistem informasi tersebut harus bekerja untuk mancapai tujuan yang telah ditentukan sebelumnya.

Sistem informasi tidak selalu sama antara perusahaan. Bergantung pada pengguna dan tujuannya, sistem informasi memiliki fungsi yang berbeda setiap penggunanya. Sistem informasi yang digunakan oleh pemakai akhir untuk penjualan berbeda dengan sistem informasi yang digunakan oleh manajer madya untuk menilai kinerja bisnis. [4]

Menurut Setiana (2011) dimulai dari tingkatan paling bawah dan tingkatan paling tinggi.

Masing-masing tingkatan sistem informasi tersebut adalah:

1. Sistem pemrosesan transaksi *(transaction processing systems)*
2. Sistem informasi manajemen *(management information systems)*
3. Sistem pendukung keputusan *(decision support systems)*

4. Sistem pakar *(artificial intelligence atau expert system)*

2.2.2 Sistem Informasi Official STT NF

Sistem Informasi manajemen konten yang dikelola oleh Sekolah Tinggi Teknologi Nurul Fikri merupakan *website* official yang menampilkan sejumlah informasi mengenai Sekolah Tinggi Teknologi Nurul Fikri. Sistem informasi tersebut diperuntukkan agar dapat diketahui oleh calon mahasiswa yang akan daftar, di dalamnya terdapat informasi-informasi yang memuat tentang program studi yang ada, informasi terkait pendaftaran, program beastudi, profil STT NF, dan yang lainnya.

Di dalam sistem informasi tersebut banyak yang dapat diakses, penjelasan secara rinci sebagai berikut:

1. Beranda

   Pada tampilan awal *website* ditampilkan beberapa informasi, yaitu mengenai informasi dan fitur-fitur yang dapat diakses seperti program studi yang ada di STT NF, informasi pendaftaran yang dialihkan ke Admisi STT NF, sitem informasi akademik yaitu elena STT NF, dan info program beastudi. Terdapat juga pengumuman terkait kalender akademik, info akademik, dan pembelajaran daring, selanjutnya terdapat berita-berita seputar kampus STT NF, serta alamat, dan kontak yang dapat dihubungi.

2. Profil

   Pada menu profil ini akan terdapat informasi tentang STT NF, visi dan misi STT NF, identitas kampus, struktur organisasi, profil dosen-dosen yang mengajar, dan informasi beberapa fasilitas yang ada di STT NF.

3. Akademik

   Informasi akademik yaitu BAAK yang mengurus administrasi STT NF, dan kemahasiswaan yang memuat organisasi, prestasi, dan semua kegiatan- kegiatan kampus.

4. Penelitian

   Menu ini menampilkan Lembaga Penelitian dan Pengabdian Kepada Masyarakat, yang mana lembaga ini bertanggung jawab dalam pengembangan penelitian dan pengabdian masyarakat.

Semua informasi yang dimuat dalam sistem informasi tersebut haruslah diamankan agar tidak terjadi keretasan data sehingga dapat disabotase oleh pihak yang tidak berwenang. Selain itu kepentingan keamanan informasi untuk menghindari ancaman yang dapat merusak sistem yang seharusnya dilindungi.

2.3 Gambaran Umum STT NF

Sekolah Tinggi Teknologi Terpadu Nurul Fikri, atau STT-NF, adalah sebuah perguruan tinggi yang menggabungkan pengetahuan tentang teknologi informasi dengan membangun individu yang islami, berbakat, dan berkarakter. Berdasarkan SK Menteri Pendidikan dan Kebudayaan Nomor 269/E/O/2012, STT-NF secara resmi didirikan pada tahun 2012.

Salah satu tujuan STT-NF adalah mencetak generasi yang berakhlak mulia, profesional dan bersertifikasi IT. Ada tiga program studi diantaranya yaitu Teknik Informatika, Sistem Informasi, dan yang terbaru Bisnis Digital. Sejauh ini STT-NF telah meluluskan sarjana-sarjana yang kompeten dan 100% terserap oleh pasar kerja.

STT-NF juga berpartisipasi dalam pengembangan perguruan tinggi untuk menghasilkan sarjana yang terpadu dengan penguasaan sains dan teknologi serta pembinaan individu yang berintegritas, kreatif, dan inovatif. STT-NF ingin menghasilkan generasi yang pintar dan bermoral. Setiap semester, mata kuliah keislaman dan kewirausahaan diberikan. *Novelty*, *Integrity*, *Care*, dan *Excellence* (NICE) ditanamkan pada setiap siswa STT-NF. Dengan kata lain, orang yang bekerja keras untuk mencapai prestasi terbaik, berusaha membuat karya yang unik dan kreatif, jujur dan berkomitmen tinggi, peduli dengan lingkungan, dan bekerja keras untuk membuat karya mereka menjadi sempurna.

2.4 Penelitian Terdahulu yang Relevan

Di bawah ini merupakan beberapa penelitian terdahulu yang menjadi rujukan atau yang menjadi penguat terhadap penelitian yang dilakukan.

Tabel 3. Penelitian Terdahulu

No	Nama dan Tahun	Judul Penelitian	Topik	Subjek	Hasil
1	**Putra, M. Y., & Tjahjadi, D. (2018)**	Evaluasi Keamanan Informasi Pada Perguruan Tinggi Bina Insani Berdasarkan Indeks Keamanan Informasi SNI ISO/IEC 27001Promosi	Evaluasi Sistem Manajemen Keamanan INformasi	Perguruan Tinggi	Hasil menunjukkan bahwa sampai saat ini, SMKI yang digunakan di Perguruan Tinggi Bina Insani menggunakan Indeks KAMI masih kurang efektif dan tidak sah.
2	**Suryono (2023)**	Evaluasi Penilaian Mandiri Penerapan SMKI di Salah satu Lingkungan K/L	*monitoring and review of ISMS*	Salah satu Lingkungan K/L	Hasil penilaian survei pemaham an SMKI antara lain perlu dilakukan pembahasan pada level OKI, khususnya forum komite SMKI untuk melakukan evaluasi beberapa komponen
3	**Enggi dan Dedy (2023)**	Assessment Risk Terhadap Penggunaan Sistem Informasi Akademik Universitas EA	*Asessment risk* dengan menggunakan kerangka pikir ISO 27001	Sistem Informasi Akademik Universitas EA	Hasil penelitian menunjukkan bahwa aset yang perlu dilindungi termasuk data dan nilai aset 11, server dan sistem informasi akademik dengan nilai aset 12.

4.	**Athallariq dan Nilo (2022)**	Penilaian Risiko pada Perusahaan dengan Berfokus pada Area Keamanan Informasi Menggunakan Iso 27001:2022	informasi digital rentan terhadap serangan siber	Perusahaan dengan Berfokus pada Area Keamanan Informasi Menggunakan Iso 27001:2022	Penerapan standar internasional ISO/IEC 27001:2013 sangat membantu perusahaan dalam memetakan berbagai risiko yang muncul terkait manajemen keamanan sistem informasi, sehingga agar risiko yang timbul dan dampaknya dapat diminimalisir dengan baik.
5	**Abdul Fattah, Bita, dan Dewi (2023)**	Penerapan Sistem Manajemen Keamanan Informasi ISO 27001 pada Perpusnas RI dalam mendukung Keamanan Tata Kelola Teknologi Informasi.	Keamanan Tata Kelola Teknologi Informasi	Perpusnas RI	berdasarkan analisis data, beberapa aset di Perpusnas teridentifikasi memiliki risiko tertentu yang tinggi. Salah satunya adalah risiko yang terkait dengan server yang tinggi disebabkan keberadaan ancaman kebakaran dan serangan hacker

Berikut ini adalah beberapa penelitian sebelumnya yang dapat digunakan sebagai referensi untuk topik penelitian ini. Penelitian ini dipilih karena terkait dengan masalah yang dibahas dalam penelitian ini dan diharapkan dapat membantu penulis dalam menyusun penelitian ini.

Pertama, penelitian oleh Putra, M. Y., & Tjahjadi, D. (2018) yang berjudul Evaluasi Keamanan Informasi Pada Perguruan Tinggi Bina Insani Berdasarkan Indeks Keamanan Informasi SNI ISO/IEC 27001. Dalam penelitian ini Perguruan Tinggi Bina Insani belum pernah melakukan pengevaluasian terhadap Sistem Manajemen Keamanan Informasi, yang mana menjadi penyebab kemudahan untuk memeroleh informasi yang tidak menutup kemungkinan munculnya ancaman baik secara fisik maupun ancaman yang berupa non fisik. Pada sisi lain lingkungan kampus terkait peningkatan data pengguna internet dan aduan ancaman yang sering terjadi adalah spam. Keamanan informasi harus diperhatikan dikarenakan penggunaan teknologi informasi yang dilakukan untuk mendukung proses bisnis. Salah satu metode yang digunakan yaitu dengan alat Indeks Keamanan Informasi (KAMI) dengan menggunakan teknik *non robability sampling* yakni *sampling* jenuh, yang berarti metode dalam pengambilan datanya dengan cara menentukan sampel yang jumlahnya sudah sesuai dengan ukuran sampel yang dijadikan sumber data sebenarnya. Dari penelitian ini menyatakan bahwa penerapan SMKI pada perguruan tersebut dengan menggunakan indeks KAMI yang mana cakupannya yaitu peran TIK, tata kelola, pengelolaan risiko, kerangka kerja, aset informasi serta teknologi keamanan informasi yang rendah dan belum *valid* yang berarti kesiapan penerapan keamanan informasi masih di bawah batas minimum yang telah dipersyaratkan oleh standar SNI ISO/IEC 27001. Dengan hasil ini didapatkan bahwa penyebabnya karena kesadaran yang dinilai cukup kurang terhadap pentingnya Sistem Manajemen Keamanan Informasi.

Kedua, penelitian oleh Suryono (2023) yang berjudul Evaluasi Penilaian Mandiri Penerapan SMKI di Salah satu Lingkungan K/L. Dalam penelitian ini disebutkan hal yang paling penting di dalam pelaksanaan SMKI adalah melakukan evaluasi terhadap pelaksanaan dan penerapan SMKI yang diistilahkan *monitoring and review of ISMS* (secara terus menerus). Dalam siklus PDCA (*Plan-Do-Check-Action*) atau biasa juga dikenal dengan *internal audit check*, evaluasi penerapan

SMKI ini mempresentasikan proses *check*. Dalam perkembangannya, evaluasi pengelolaan keamanan informasi bagi penyelengara pelayanan yang berdasarkan Panduan Penerapan Tata Kelola Keamanan Informasi dalam Penyelenggara Pelayanan Publik dengan alat evaluasi yang berupa penggunaan Indeks Keamanan Informasi (Indeks KAMI). Tujuan dari evaluasi penerapan SMKI ini selain sebagai tindak lanjut dari nota dinas (280/PID.00/30- 32/10/2022) yang diturunkan dari Tim Inspektorat, yaitu untuk mendapat penilaian yang mengenai pengelolaan keamanan TI di dalam lingkungan lembaga, kedua untuk mengetahui tingkat pemahaman serta kematangan dalam pengelolaan keamanan TI dan mendapatkan rekomendasi yang berdasar pada hasil analisis pengelolaan keamanan informasi pada Lembaga Awdx. Metode yang digunakan adalah mengumpulkan, menggolongkan, dan menganalisis data yang berupa angka untuk mendapatkan informasi dalam mengukur pemahaman struktur dan implementasi SMKI. Metode ini merupakan metode kuantitatif survei yang berangkat dari permasalahan yang terdiri atas latar belakang masalah, identifikasi masalah, serta rumusan masalah. Permasalahan tersebut selanjutnya dijelaskan dan dijawab dengan teori. Secara menyeluruh dari hasil penilaian survei pemahaman SMKI antara lain perlu dilakukan pembahasan pada level OKI, khususnya forum komite SMKI untuk melakukan evaluasi beberapa komponen pada aspek pengendalian dan aspek organisasi keamanan informasi. Kegiatan penilaian atau evaluasi harus dilakukan berkelanjutan minimal setahun sekali sebagai bentuk kontrol sistem manajemen.

Ketiga, penelitian oleh Enggi dan Dedy (2023) yang berjudul Assessment Risk Terhadap Penggunaan Sistem Informasi Akademik Universitas EA Menggunakan Metode ISO 27001. Dalam penelitian ini diketahui bahwa Sistem Informasi Akademik (SISFO) di Universitas EA terdiri yang terdiri dari berbagai macam komponen didalamnya, seperti *hardware, software,* sumber daya manusia, dan juga sarana pendukungnya. Diketahui bahwa sampai saat ini bagian Divisi TI dapat dikatakan belum meyeluruh dalam melakukan kontrol analisa yang menjadi penyebab terjadinya permaslahan yang muncul pada aset TI yang mengakibatkan server sering mengalami *down* secara mendadak yang disebabkan oleh listrik yang mati dan suhu ruangan yang panas, kurangnya kesadaran untuk melakukan *backup* data baik data dalam aplikasi maupun database, operasional penggunaan SISFO

yang salah, pengawasan yang kurang dalam proses update sistem aplikasi serta buka tutup port-*port* pada server yang tidak hati-hati, keamanan (*firewall)* yang tidak bekerja pada server, pengawasan yang dinilai kurang ada penggunaan hak akses serta memonitoring *bugs* dan *error* pada aplikasi secara berkala. Metodologi yang digunakan paad penelitian ini yaitu penelitian kualitatif dengan pendekatan deskriptif. Pengumpulan datanya yaitu melalui observasi, wawancara, dan studi pustaka, artinya penelitian ini dimulai dengan pengumpulan beberapa data kejadian atau gangguan yang terjadi. Data yang diteliti yaitu berupa aset yang berikutnya dianalisa dengan tahapan *assesment risk* menggunakan kerangka pikir ISO 27001. Hasil dari penelitian ini yaitu terdapa beberapa aset yang harus dilindungi datanya dengan nilai aset 11, server dan sistem informasi akademik dengan nilai akses 12, dan kemudian melakukan evaluasi level risiko yang bernilai tinggi dengann menentukan penanganan risiko yang berupa dokumen penilaian beserta penyusunan kontrol risiko guna menjamin keamanan pada aset TI.

Keempat, penelitian oleh Athallariq dan Nilo (2022) yang berjudul Penilaian Risiko pada Perusahaan dengan Berfokus pada Area Keamanan Informasi Menggunakan Iso 27001:2022. Dalam penelitian tersebut dipaparkan bahwa semua informasi digital rentan terhadap serangan *cyber*. Menurut proyek *honeynet* dari BSSN, terdapat 9,6% lebih banyak serangan *cyber* di Indonesia pada tahun 2021 dibandingkan tahun 2020. *Ransomware* dan pelanggaran data merupakan dua jenis serangan *cyber* yang sering terjadi. Oleh karenanya dalam mengelola masalah keamanan ini, perusahaan perlu mengadopsi strategi keamanan informasi dengan cara menciptakan kerangka kerja yang lengkap untuk memungkinkan pengembangan, pelembagaan, penilaian, dan peningkatan program keamanan informasi. Rencana strategis organisasi harus didukung oleh strategi keamanan informasi secara luas dengan konten yang ditelusuri kembali ke sumber-sumber tingkat yang lebih tinggi. Menurutnya, serangan *cyber* adalah serangan terhadap komputer atau jaringan telekomunikasi terhadap komputer atau jaringan telekomunikasi lain, misalnya situs web. Secara internal, Perusahaan IT Software masih memiliki banyak kelemahan keamanan informasi. Risiko keamanan informasi, khususnya pada perusahaan berbasis teknologi informasi, cukup besar. Oleh karena itu, Perseroan perlu memperhatikan risiko terkait SMKI. Standar

ISO/IEC 27001 sering digunakan untuk mengidentifikasi apakah keamanan sistem informasi harus diterapkan. Untuk membuat Sistem Manajemen Keamanan Informasi (SMKI), perlu mematuhi persyaratan yang diuraikan dalam ISO/IEC 27001:2022. Metode penerapannya didasarkan pada SNI ISO/IEC 27001:2022 dan dipadukan dengan penilaian risiko pada ISO/IEC 31000:2013. Dalam SNI ISO/IEC 27001:2022, penulis mengacu pada klausul 9 (Evaluasi Kinerja). Dalam penilaian risiko pada SNI ISO/IEC 31000:2018, penulis mengacu pada penilaian risiko yang terbagi dalam tiga tahap (Identifikasi Risiko, Analisis Risiko, dan Evaluasi Risiko). Berdasarkan hasil penelitian dapat diambil beberapa kesimpulan yaitu, penilaian risiko Perusahaan IT Software untuk fokus aplikasi perangkat lunak bisnis menunjukkan bahwa 86,87% risiko teridentifikasi sebagai risiko rendah, 6,06% sebagai risiko Sedang , dan 7,07% berisiko tinggi. Berdasarkan kategori keamanan, data pelanggan pada Perusahaan IT Software termasuk dalam kategori aman. Hal ini ditunjukkan dengan total risiko medium sebanyak enam dan total risiko *High* sebesar 7. Penerapan standar internasional ISO/IEC 27001:2013 sangat membantu perusahaan dalam memetakan berbagai risiko yang muncul terkait manajemen keamanan sistem informasi, sehingga agar risiko yang timbul dan dampaknya dapat diminimalisir dengan baik. Berdasarkan hasil penelitian yang telah disimpulkan, terdapat saran untuk penelitian selanjutnya agar penilaian risiko yang telah dilakukan dapat diukur terhadap sisa risiko-risiko yang telah dimitigasi terhadap risiko yang telah dipetakan dengan SNI ISO/IEC 27001: 2022. Hal ini diperlukan guna mengukur risiko-risiko yang telah dimitigasi untuk mengetahui efektivitas penerapannya dalam suatu organisasi.

Kelima, penelitian oleh Abdul Fattah, Bita, dan Dewi (2023) yang berjudul Penerapan Sistem Manajemen Keamanan Informasi SNI ISO/IEC 27001 pada Perpusnas RI dalam mendukung Keamanan Tata Kelola Teknologi Informasi. Dalam penelitian tersebut disebutkan bahwa Sistem informasi juga memiliki berbagai risiko seperti gangguan pasokan listrik, kesalahan manusia, pencurian data oleh peretas, kerusakan sistem akibat serangan virus, dan lainnya. Untuk mengurangi risiko, diperlukan praktik tata kelola risiko yang baik dan efektif. Tahapan alur penelitian tersebut meliputi Studi Literatur, Identifikasi Masalah, Observasi dan Wawancara, Menggumpulkan Data, Mengelompokkan Data dan

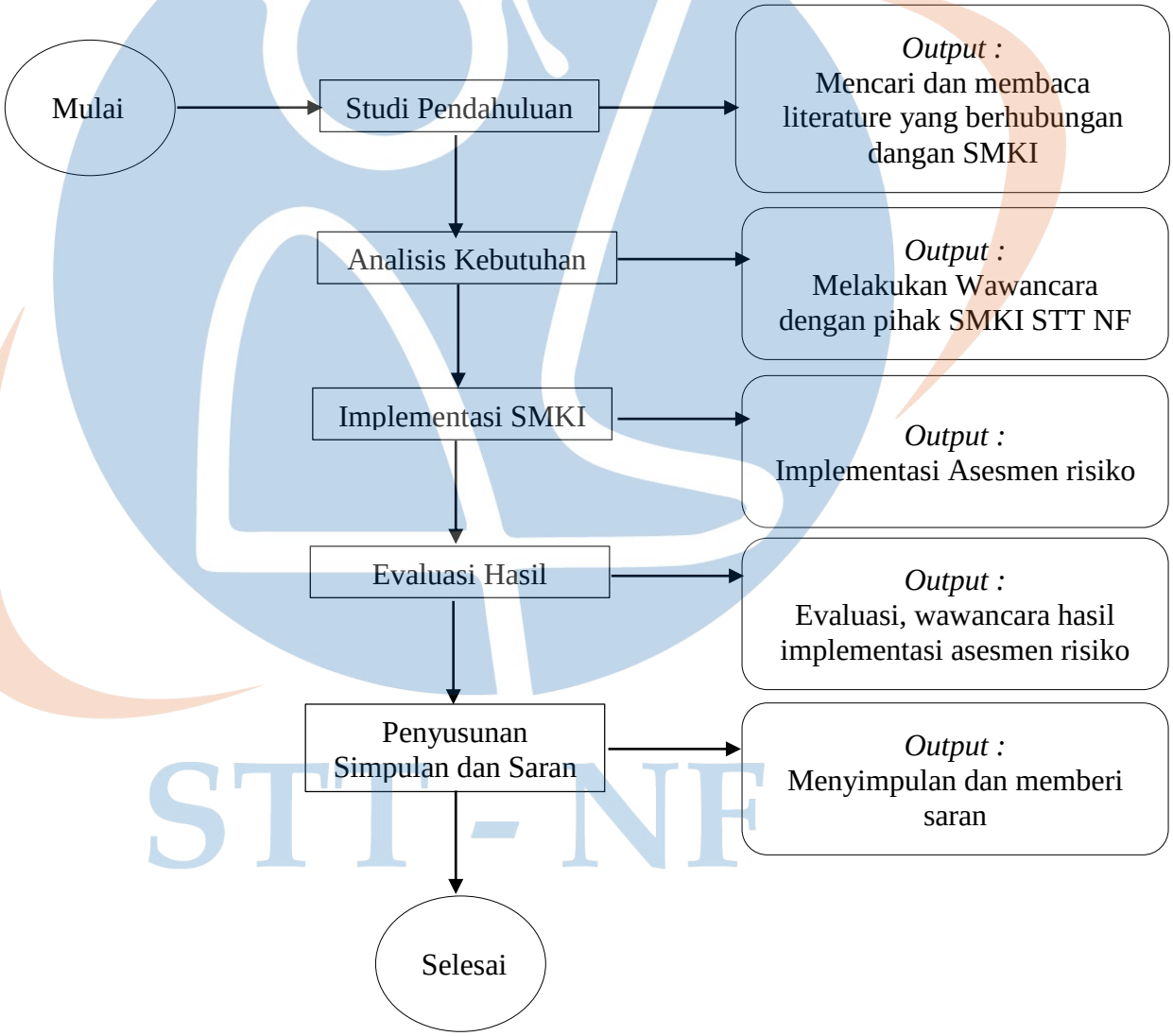
Menganalisis Data, Rekomendasi Hasil, Kesimpulan dan rekomendasi. Hasil dari penelitian ini berdasarkan analisis data, beberapa aset di Perpusnas teridentifikasi memiliki risiko tertentu yang tinggi. Salah satunya adalah risiko yang terkait dengan server yang tinggi disebabkan keberadaan ancaman kebakaran dan serangan *hacker* merupakan faktor yang masih menjadi penyebab utama belum adanya kekurangan dalam sistem pendeteksi dini kebakaran dan kurangnya pemantauan dalam pengelolaan informasi. Sedangkan untuk semua server belum tersedia kembali server *backup*.

BAB III
METODOLOGI PENELITIAN

Pada bab ini yaitu akan dijelaskan terkait metode penelitian dan pengambilan data, serta tahapan-tahapan yang dilalui dalam proses penelitian ini.

3.1 Tahapan Penelitian

Pada bagian ini yang mana menjelaskan tahapan tahapan yang disajikan dalam gambar di bawah ini.



Gambar 1. Tahapan Penelitian

3.1.1 Studi Pendahuluan

Pada tahapan ini dilakukan studi guna mendapatkan data data yang dibutuhkan dalam menulis penelitian, yaitu dengan studi literatur yang mana dalam tahapan ini mengkaji mengenai teori yang mendukung dalam melakukan penelitian. Sehingga dapat membantu peneliti menentukan metode-metode yang digunakan dalam penelitian ini. Studi pendahuluan dengan mencari dan membaca literatur yang berhubungan dengan SMKI yang mengacu pada dokumen SNI ISI/IEC 27001. Dalam tahap ini yaitu mencari beberapa referensi yang mana dapat membantu dalam menyusun penelitian ini.

3.1.2 Analisis Kebutuhan

Dalam tahap ini yaitu melakukan upaya untuk mengumpulkan data-data yang dibutuhkan, seperti hasil wawancara, hasil observasi, dan kajian literatur. Mengidentifikasi apa saja yang harus dilengkapi agar tidak mendapat ancaman. Wawancara dalam upaya untuk memenuhi kebutuhan dalam penelitian ini yaitu dilakukan dengan pihak terkait bagian pengelola dan keamanan *website* kampus STT NF.

3.1.3 Implementasi SMKI

Setelah menganalisis apa saja yang dibutuhkan dalam penelitian ini, tahap selanjutnya yaitu melakukan implementasi sesuai dengan analisis kebutuhan. Hal-hal yang akan diimplementasikan yaitu sampai proses asesmen risiko keamanan informasi. Tugas akhir ini tidak melaksanakan implementasi hingga penanganan risiko dan pelaksanaan kontrol keamanan.

3.1.4 Evaluasi Hasil

Tahap selanjutnya yaitu membahas tentang evaluasi hasil, yang mana dalam tahap ini akan dilakukan evaluasi. Evaluasi dilakukan dengan kembali melakukan wawancara untuk evaluasi terkait asesmen risiko yang telah dilakukan. Sehingga ddidapatkan hal apa saja yang dapat dihasilkan kesimpulan terkait asesmen risiko tersebut.

3.1.5 Penyusunan Kesimpulan dan Saran

Tahapan akhir yaitu penyususnan kesimpulan dan saran, yang mana dalam bagian ini tentu sudah dapat menyimpulan tentang hasil yang diperoleh. Dalam penelitian ini yaitu dengan mengimplementasikan serta mengevaluasi Sistem Manajemen Keamanan Informasi (SMKI) dengan SNI ISO/IEC 27001:2022. Yang bertujuan dapat memberikan solusi, serta memberi saran agar dapat dilanjutkan kembali.

3.2 Rancangan Penelitian

3.2.1 Jenis Penelitian

Jenis penelitian yang digunakan yaitu penelitian eksploratif yang digunakan untuk menjelaskan masalah apa yang harus diselesaikan dan apa yang harus dilakukan dalam penelitian selanjutnya. Dalam hal tersebut proses implementasi dan evaluasi berdasar kepada hasil dari wawancara yang dilakukan dengan pengelola website implementasi Sistem Manajemen Keamanan Informasi (SMKI) yang mengacu pada dokumen SNI ISO/IEC 27001:2022. Penelitian ini dibatasi hanya sampai dengan asesmen risiko keamanan informasi dan tidak melaksanakan implementasi hingga penanganan risiko dan pelaksanaan kontrol keamanan.

3.2.2 Metode Analisis Data

Metode analisis data dalam penelitian ini yaitu analisis kualitatif. Analisis kualitatif adalah proses mengumpulkan dan mencari serta menyusun secara sistematis data yang telah diperoleh dari hasil wawancara. Hasil dari wawancara tersebut menjadi sumber data yang dituangkan dalam penelitian.

3.2.3 Metode Pengumpulan Data

Metode yang digunakan yaitu dengan metode kualitatif, yang mana pengambilan data tersebut dengan wawancara dan menguraikan secara apa adanya. Uraian masalahnya tidak dengan ukuran pasti atau mutlak yang bersifat relatif, perasaan, dan lain-lain, yaitu dengan wawancara yang telah diajukan beberapa pertanyaan. Pengumpulan data ini didapatkan dari hasil wawancara yang dilakukan dengan pengelola *website official* STT NF untuk mendapatkan data keretasan yang terjadi.

3.2.4 Metode Pengujian Evaluasi

Pengujian evaluasi dengan melakukan wawancara kembali dengan pihak terkait yaitu pengelola *website official* STT NF yang dilakukan untuk mengevaluasi hasil asesmen risiko yang telah dilakukan dengan beberapa tahapan implementasi asesmen risiko yang dapat menjadi pertimbangan untuk pengimplementasian standar keamanan informasi lebih lanjut dengan tujuan untuk menjaga sistem keamanan informasi dari kerentanan dan ancaman yang mungkin bisa terjadi lagi.

3.3 Kebutuhan Sarana dan Prasarana

Adapun sarana dan prasarana yang dibutuhkan dalam penelitian ini diantara lain:

1. Laptop Lenovo K21-80
    a. Tipe Processor Intel Core i3
    b. RAM : 4.00 GB
    c. Sistem Operasi : Windows 10
2. Software yang digunakan :
    a. Microsoft Word 2010
    b. Microsoft Excel 2010
    c. Google Chrome

BAB IV
HASIL DAN PEMBAHASAN

4.1 Analisis Kebutuhan

Dalam proses penelitian ini tahapan yang penting sebelum melakukan asesmen risiko yaitu dengan menggali lebih dalam tentang sistem informasi *official* STT NF dengan melakukan wawancara dengan pengelola *website* tersebut sehingga didapatkanlah informasi yang menjadi bahan penelitian untuk melakukan asesmen risiko.

Pada tahapan ini dilakukan wawancara untuk memenuhi kebutuhan penelitian yang mana diantaranya untuk mendapatkan informasi untuk memenuhi kebutuhan dalam penelitian ini. Seperti yang telah diketahui bahwa sistem informasi *official* STT NF ini merupakan sebuah halaman yang menampilkan informasi terkait kampus STT NF yang mana mesti dijaga kerahasiaan, keintegritasan, maupun ketersediaan agar dapat beroperasi dengan baik tanpa gangguan dan ancaman apapun.

Setelah dilakukan wawancara terkait penerapan standar keamanann informasi pada *website official* STT NF didapatkan informasi bahwa sistem informasi tersebut belum menerapkan keamanan informasi yang berstandar nasiolan SNI ISO/IEC 27001, alasannya karena ketidak tahuan informasi terkait standar keamanan informasi guna melindungi asset dan data informasi yang bersifat rahasia dan terhidar dari berbagai ancaman yang sewaktu-waktu dapat terjadi seperti peretasann dan lain-lain yang tentunya dapat mengganggu jalannya sistem informasi tersebut sehingga tidak dapat berjalan atau beroperasi dengan baik.

Dari hasil wawancara tersebut juga dikatakan bahwa pernah terjadi serangan *malware* yang pada sistem informasi *official* STT NF, yang mana pada saat itu sangat mengganggu jalannya sistem informasi tersebut dan berdampak pada penggunaan atau keberlangsungan sistem informasi yang tidak dapat beroperasi dengan baik.

Malware merupakan sebuah perangkat lunak yang mana dapat merusak sistem, server, maupun jaringan dalam komputer yang bekerja dengan memasuki komputer tanpa adanya perizinan. *Malware* ini merupakan suatu perangkat lunak

yang jahat dan berbahaya yang dapat menjadi pintu bagi para peretas atau biasa disebut *hacker* untuk mencuri data informasi yang tersimpan dalam komputer.

Dampak dari serangan *malware* tersebut tentu sangat mengganggu jalannya sebuah sistem informasi. Rusaknya sistem, server, dan jaringan komputer dapat menyebabkan sistem informasi tersebut tidak dapat bekerja atau berjalan secara optimal atau bahkan tidak dapat diakses oleh pengguna lain, selain itu juga dapat terjadi *error*. Sistem informasi tersebut tidak beroperasi dengan semestinya seperti sistem tidak menampilkan halaman yang sesuai dengan pilihan halaman yang dipilih oleh pengguna.

Untuk mengatasi serangan *malware* tersebut langkah awal yang dilakukan yaitu dengan melakukan pemindaian untuk mengetahui keberadaan *malware* pada sistem informasi tersebut. Dapat juga mendeteksi dokumen atau data mana yang telah terinfeksi oleh *malware* tersebut. Yang kedua dengan melakukan pencadangan *website* tersebut sebelum terinfeksi *malware* sebagai tindakan pencegahan.

Dalam kasus ini, terjadinya *malware* tentu sangat berkaitan dengan Sistem Manajemen Keamanan Informasi. Penerapan standar keamanan informasi dipastikan dapat mengamankan sebuah sistem informasi terhidar dari serangan *malware* tersebut. Karena dalam penerapan standar keamanan nasional terdapat tiga aspek utama yang digunakan untuk penerapan standar keamanan informasi diantaranya yaitu, *confidentiality* (kerahasiaan), *integrity* (integritas), dan *avaibility* (ketersediaan).

Tiga aspek tersebut tentunya dapat mencegah terjadinya serangang pada server maupun lainnya, karena dengan adanya aspek tersebut sebuah sistem informasi dapat terjamin keamanan data yang ada pada sistem informasi tersebut. Juga didukung oleh dokumen penerapan Sistem Manajemen Keamanan Informasi yang mengatur terkait penerapan standar keamanan tersebut.

4.2 Asesmen Risiko SMKI

Dari hasil wawancara yang telah dilaksanakan dengan pengelola *website official* STT NF bahwa pada sistem informasi tersebut belum menerapkan Sistem Manajemen Keamanan Informasi (SMKI) yang berstandar nasional SNI ISO/IEC 27001. Hal ini disebabkan karena kurangnya informasi terkait standar keamanan

informasi tersebut. Selama sistem informasi tersebut beroperasi terjadi kasus yang menimbulkan dampak yang tinggi karena sistem informasi tersebut mengalami kerentanan yaitu serangan *malware*. Tentu dengan terjadinya hal tersebut sangat mengganggu jalannya sistem informasi tersebut.

Terjadinya serangan *malware* ini tentu saja dipicu karena tidak diterapkannya keamanan yang berstandar nasional diterapkan dalam sistem informasi tersebut. Serangan *malware* yang terjadi pada sistem informasi tersebut terkena dari sisi server yang menggunakan keamanan dari provider. Dampaknya yaitu terganggunya operasional dari *website official* STT NF yang mana ketika terjadi *malware* tersebut, *website* tidak bisa berjalan baik yang pada saat itu sistem tidak bisa diakses oleh *user* luar atau lembaga lain, dan sistem tidak menampilkan halaman yang sesuai dengan halaman pilihan pengguna. Dampak terjadi gangguan tersebut dapat teratasi selama lima hari sistem informasi baru sistem digunakan kembali. Berikut tahapan-tahapan implementasi asesmen risiko pada *website official* STT NF :

1. Tahap Pertama

   Tahapan pertama dari hasil wawancara didapatkan bahwa kriteria nilai kemungkinan dan nilai dampak. Nilai kemungkinan diperoleh Nilai 2 (rendah/kecil) karena kemungkinan terjadi 1x dalam setahun hingga dua tahun. Nilai dampak diperoleh Nilai 5 (sangat tinggi) karena pekerjaan tertunda selama enam jam atau lebih.

2. Tahap Kedua

   Dalam kasus yang terjadi di atas yaitu serangan *malware* yang terjadi nilai kemungkinannya yaitu 2, karena kemungkinan terjadi 1x dalam setahun hingga dua tahun. Akan tetapi untuk nilai dampaknya yaitu 5 karena sistem informasi tidak dapat digunakan atau diakses selama lima hari. Jumlah perkalian dari kemungkinan dan dampak tersebut yaitu 2 x 5 yang menghasilkan 10, sehingga dengan table kriteria diatas termasuk kategori yang tinggi.

3. Tahap Ketiga

   Penentuan keberterimaan risiko yang telah dilakukan asesmen risiko pada tahap kedua. Dinyatakan bahwa kriteria asesmen risiko tergolong tinggi

karena nilai kriterianya didapatkan 10. Maka dapat dipastikan bahwa risiko tidak dapat diterima.

4. Tahap Akhir

   Berdasarkan hasil dari tahap ke tiga yang mana level keberterimaan risiko yang terjadi pada sistem informasi *website official* STT NF yang mana level risikonya tergolong tinggi. Sehingga untuk penanganan risiko ini menjadi prioritas utama yang harus segera ditangani. Berikut hasil dari asesmen risiko yang telah dilakukan dengan sumber data berdasarkan kerentanan yang terjadi.

Tabel 4. Hasil Asesmen Risiko

No		1
Asset Classification	Klasifikasi asey sesuai dengan Lampiran A; Organisasi, Orang, Fisik, dan Teknologi	Teknologi
Dept	Tempat Assesmen risiko atau pemilik risiko	Bagian IT
Nama Aset		Software : Sistem Informasi Official STT NF
Vulnerability	Kerentanan atau keleahan aset dari sisi keamanan informasi	Serangan Malware dari sisi server
Threat	Ancaman dari dalam atau luar organisasi terhadap kerentanan	dapat merusak server, peretasan data, sistem tidak dapat diakses
Impact (Dampak Ancaman yang dirugikan)	**C** : confidentiality **I**: Integrity **A**: Avaibility	**C** : confidentiality **I**: Integrity **A**: Avaibility
Likelihood (Peluang Terjadi)	0 s.d 5	2
Severity (Dampak Kerugian)	0 s.d 5	5
Nilai Risiko dalam angka	Likehold x Severity (Peluang x Dampak kerugian)	10
Nilai Risiko dalam Teks	1-4 Rendah, 5-9 Sedang , 10 - 16 Tinggi , > 16 Sangat Tinggi	Tinggi

4.3 Evaluasi Hasil

Dari tahapan-tahapan yang telah dilakukan di atas dan diperoleh hasil yaitu nilai kemungkinannya yaitu 2 dan nilai dampaknya yaitu 5. Sehingga diperoleh nilai kriteria risikonya dari hasil perkalian antara nilai kemungkinan dan nilai dampak yaitu 2x5 = 10. Maka dapat ditentukan bahwa nilai kriteria termasuk

golongan yang tinggi atau termasuk level risiko yang tinggi dan keberterimaan risiko tidak dapat diterima karena mengganggu kinerja sistem informasi lebih dari satu hari.

Dengan hasil ini maka dilakukan kembali wawancara evaluasi terkait asesmen risiko yang telah dilakukan. Maka dari itu untuk sistem informasi *website official* STT NF ini dianjurkan untuk menerapkan sistem manajemenn keamanan informasi yang mana dalam penerapannnya dapat menjaga kestabilan dan keamanan yang terjamin karena menggunakan standar keamanan nasional. Dapat dilihat dari tabel hasil asesmen risiko di atas yang mana ancaman yang terjadi dapat merusak server, peretasan data, juga sistem tidak dapat diakses yang menjadi kendala atau gangguan yang menjadi pemicu sistem informasi tersebut tidak bisa beroperasi secara normal. Keadaan ini tentu dapat mengganggu *confidentiality* (kerahasiaan), *Integrity* (Integritas), dan *avaibility* (ketersediaan) yang dapat mengancam kestabilan *website* tersebut. Dalam kasus ini yang mana terjadi serangan *malware* yang berdampak sangat merugikan bagi kampus STT NF terutama pada *website official* STT NF. Pertama dalam hal kerahasian tentu dapat terancam karena sengan *malware* tersebut sangat dapat mengganggu dan bisa terjadi pencurian dan peretasan data. Kedua, keintegritasan isi dalam *website* tersebut yang dapat terjadi manipulasi data dan perubahan data yang dilakukan oleh pihak yang tidak berwenang untuk melakukan perubahan informasi atau data yang ada dalam *website official* STT NF. Ketiga, ketersediaan informasi yang mana dalam kasus ini ketersediaan *website official* STT NF terganggu sampai terjadi *error* yang menyebabkan *website* tersebut tidak bisa menampilkan halaman yang diinginkan oleh penguna.

Kerentanan yang pernah terjadi mungkin saja dapat terulang kembali, maka dari itu menganjurkan untuk menerapkan standar keamanan informasi yang telah dilakukan implementasi asesmen risiko yang menjadi tahap awal untuk penerapan standar keamanan sistem informasi tersebut. Namun, dari hasil wawancara dikatakan untuk saat ini sudah cukup terbilang masih aman dan terkendali oleh aturan yang dibuat untuk *hardening security* dari sisi internal dan *provider*.

Hasil dari analisis penerapan Sistem Manajemen Keamanan Informasi (SMKI) pada *website official* STT NF ini tentu masih banyak kekurangan, yang

mana dalam batasan analisis pun yang hanya dilakukan sampai proses asesmen risiko, sehingga penelitian ini perlu adanya lanjutan hingga sampai tahapan akhir untuk penerapan Sistem Manajemen Keamanan Informasi (SMKI) yang berstandar nasional.

Dari hasil asesmen risiko yang mungkin belum lengkap dan masih perlu mengidentifikasi kembali risiko-risiko yang terjadi. Sehingga belum dapat dijadikan patokan untuk risiko yang dapat berdampak besar untuk sistem informasi tersebut dan perlu menggali kembali risiko yang terjadi serta menentukan kemungkinan dan dampak yang akan ditimbulkan. Pengujian evaluasi yang dilakukan pun hanya dengan pengelola *website official* STT NF saja, yang seharusnya melibatkan beberapa orang yang terlibat dalam pengelolaan *website* tersebut, dan disarankan untuk penelitian ini dapat dilanjutkan dikemudian waktu.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Proses wawancara sebagai langkah awal untuk dapat mengimplementasikan proses asesmen risiko untuk menggali aset yang terancam sehingga mengganggu operasional dan berdampak tidak berjalan dengan baik. Seperti yang diketahui bahwa sistem informasi *official* STT NF ini merupakan sebuah halaman yang menampilkan informasi terkait kampus STT NF. Sistem informasi tersebut mesti dijaga kerahasiaan, keintegritasan, maupun ketersediaannya agar dapat beroperasi dengan baik tanpa gangguan dan ancaman apapun. Dari hasil wawancara telah didapatkan bahwa aset tersebut yaitu sistem informasi terkena serangan *malware* yang menyebabkan *website* tersebut tidak bisa digunakan atau tidak berjalan dengan normal. Dampak yang ditimbulkan berisiko tinggi yang mana dapat merusak server, peretasan data, dan sistem tidak dapat diakses. *Website* tidak dapat diakses dan terjadi *error*, diantaranya sistem tidak dapat menampilkan halaman yang sesuai dengan halaman pilihan pengguna. Ancaman risiko tersebut kemungkinan terjadi dalam jangka waktu satu tahun atau kurang dari dua tahun, serta dampak yang ditimbulkan ternilai tinggi. Kerentanan risiko tersebut ternilai tinggi karena terjadi kerentanan tersebut mengganggu operasional *website* selama lima hari dan dapat ditetapkan bahwa risiko tersebut tidak dapat diterima.

Setelah dilakukan asesmen risiko, maka selanjutnya yaitu mengevaluasi hasil dari hasil asesmen risiko dengan melakukan wawancara kembali dengan pihak pengelola *website* STT NF. Kerentanan yang pernah terjadi mungkin saja dapat terjadi kembali, karena ancamannya dapat mengganggu operasional sistem informasi yang meliputi *confidentiality, integrity & avaibility.* Kerahasiaan (*confidentiality)* daoat terganggu karena ancaman rusaknya server sistem informasi tersebut, integritas (*integrity)* dapat terganggu yang mana dapat terjadi peretasan data dan perubahan data oleh pihak tidak berwenang, dan ketersediaan (*avaibility)* juga dapat terganggu karena sistem tidak dapat diakses. Dengan hasil pengimplementasian asesmen risiko ini telah dilakukan evaluasi dengan hasil dari asesmen risiko yang telah dijalankan dapat membantu pengelola *website official*

STT NF untuk mengetahui terkait standar keamanan informasi ini yang mana sebelumnya tidak diterapkannya standar keamanan informasi ini karena ketidaktahuan terhadap standar keamanan nasional SNI ISO/IEC 27001:2022 ini. Walaupun untuk saat ini keamanan sistem informasi tersebut masih terbilang cukup aman dengan adanya penggunaan keamanan yang digunakan oleh *provider* yang mana untuk pencegahan yang dianjurkan untuk menerapkan SMKI masih sudah cukup dengan dibuatnya aturan untuk *hardering security* dari sisi internal dan *provider*. Melihat dari hasil asesmen yang didapatkan bahwa risiko yang terjadi tergolong tinggi sehingga untuk mencegah terjadinya kembali maka penerapan Sistem Manajemen Keamanan Informasi (SMKI) yang berstandar nasional disarankan untuk menjamin keamanan informasi.

5.2 Saran

Penerapan Sistem Manajemen Keamanan Informasi (SMKI) yang dilakukan pada *website official* STT NF ini hanya dilakukan sampai proses asesmen risiko, tentu saja hasilnya mungkin belum lengkap dan perlu mengidentifikasi kembali risiko yang terjadi. Oleh karena itu, tidak dapat digunakan sebagai patokan dan perlu menggali kembali risiko yang telah terjadi dan menentukan kemungkinan dan konsekuensi dari risiko tersebut. Ancaman atau kerentanan yang terjadi dapat mengganggu kestabilan sitem informasi tersebut dari segi kerahasiaan (*confidentiality)* agar tidak terjadi rusaknya sever, integritas (*integrity)* yang dapat terjadi peretasan data dan perubahan oleh pihak yang tidak berwenang, dan ketersediaan (*avaibility)* yang dapat mengganggu operasional sistem informasi tersebut.

Pengujian evaluasi yang dilakukan pun hanya melibatkan pengelola *website official* STT NF, yang seharusnya melibatkan orang lain yang terlibat dalam pengelolaan *website* tersebut seperti pihak pengelola server dari sistem informasi tersebut yaitu LTSI STT NF. Oleh karena itu, disarankan agar penelitian ini dilanjutkan untuk dapat sampai pada proses akhir dengan urutan tahapan asesmen risiko sampai dengan audit internal, sehingga penilaian terhadap penerapan Sistem Manajemen Keamananan Informasi (SMKI) lengkap dan dapat diajukan untuk penerapan standar keamanan informasi SNI ISO/IEC 27001:2022.

DAFTAR PUSTAKA

[1] M. U. Dewi, "sistem-informasi-s1.stekom.ac.id," 27 January 2022. [Online]. Available: https://sistem-informasi- s1.stekom.ac.id/informasi/baca/Sistem-Manajemen-Keamanan-Informasi/6010bc6d1b32ea28db247cf5591745c15edfa6e6.

[2] Rhenn, "dosenit.com," Mengenal Sistem Manajemen Keamanan Informasi, 2023. [Online]. Available: https://dosenit.com/ilmu-komputer/sistem-manajemen-keamanan- informasi. [Accessed 25 May 2023].

[3] N. A. Setyaningsih, "kemenkeu.co.id," kemenkeu, 16 September 2022. [Online]. Available: https://klc2.kemenkeu.go.id/kms/knowledge/berkenalan-dengan- sistem-manajemen-keamanan-informasi-smki-dalam-iso-27001-2013-371a0e07/detail/. [Accessed 23 May 2023].

[4] A. Irfansyah, "ISO 27001 dan CIA Triad, Apa Hubungannya dalam Keamanan Informasi?," https://eduparx.id/, 20 September 2023. [Online]. Available: https://eduparx.id/blog/insight/hubungan-iso-27001-dan-cia-triad-dalam-keamanan-informasi/. [Accessed 21 Juny 2024].

[5] I. Consulting, "Ketahui 6 Langkah Penilaian dan Penanganan Risiko dalam ISO 27001," https://integrasolusi.com/, 9 February 2023. [Online]. Available: https://integrasolusi.com/blog/ketahui-6-langkah-penilaian-dan-penanganan-risiko-dalam-iso-27001/. [Accessed 21 Juny 2024].

[6] A. R. Setiana, "adirobith.blogspot.com," blogspot.com, 11 November 2011. [Online]. Available: http://adirobith.blogspot.com/2011/11/rpp.html. [Accessed 25 May 2023].

[7] M. S. Islam, "Tujuan Keamanan Informasi dan Legitimasi Keluaran ISO/IEC 27001," Springer Link, 21 August 2023. [Online]. Available: https://link.springer.com/article/10.1007/s10257-023-00646-y. [Accessed 22 April 2024].

[8] D. L. Fajri, "katadata.co.id," 21 Juny 2023. [Online]. Available: https://katadata.co.id/lifestyle/edukasi/6492a0d1a4b93/pengertian-rumus-dan-cara-menghitung-skala-likert.

[9] Asfihan, "ruangpengetahuan.co.id," 23 May 2023. [Online]. Available: https://ruangpengetahuan.co.id/pengertian-sistem-informasi/.

[10] V. Zwass, "www.britannica.com," Britannica, 20 May 2023. [Online]. Available: https://www.britannica.com/topic/information-system/Computer-software. [Accessed 23 May 2023].

[11] I. Suryono, "ISMS EVALUASI PENILAIAN MANDIRI PENERAPAN SMKI DI LINGKUNGAN LEMBAGA AWDX," *Evaluasi Implementasi SMKI*, vol. 1, p. 1, 2019.

[12] M. Y. &. T. D. Putra, "Evaluasi Keamanan Informasi Pada Perguruan Tinggi Bina Insani Berdasarkan Indeks Keamanan Informasi SNI ISO/IEC 27001.," *Penelitian Ilmu Komputer Sistem Embedded and Logic*, vol. 6, no. 1, pp. 95-104, 2018.

[13] D. S. Enggi Ardius, "ASSESMENT RISK TERHADAP PENGGUNAAN SISTEM INFORMASI AKADEMIK UNIVERSITAS EA MENGGUNAKAN METODE ISO 27001," *Jurnal Teknologi Informasi Mura*, vol. 15, pp. 1-5, 2023.

[14] N. A. K. F. Hafizh Ghozie Afiansyah, "Penyusunan kebijakan Pengamanan dan Pengelolaan Infrastruktur Operasi Keamanan Siber Menggunakan NIST CSF 2.0 dan ISO/IEC 27001:2022," *Jurnal Info Kripto*, vol. 17, no. 3, pp. 95-96, 2023.

[15] B. P. Z. D. E. W. Moh. Abdul Fattah Ys, "Penerapan Sistem Keamanan Informasi ISO 27001 Pada Perpusnas RI dalam mendukung Keamanan Tata Kelola Teknologi Informasi," *Cyber Security dan Forensik Digital*, vol. 6, p. 76, 2023.

[16] A. Tholchah, "Pahami Risiko Keamanan Informasi dengan ISO 27001," PT SINERGI INFORMATIKA SEMEN INDONESIA, 3 November 2023. [Online]. Available: https://sisi.id/stories/insight/pahami-risiko-keamanan-informasi-dengan-iso-27001/. [Accessed 21 Juny 2024].

[17] ITG.ID, "6 Langkah Penilaian Risiko dalam ISO 27001," ITG.ID, 28 December 2018. [Online]. Available: https://itgid.org/6-langkah-penilaian-risiko-dalam-iso-27001/. [Accessed 21 Juny 2024].

[18] I. T. Solusi, "Ketahui 6 Langkah Penilaian dan Penanganan Risiko dalam ISO 27001," Integra Teknologi Solusi, 9 February 2023. [Online]. Available: https://integrasolusi.com/blog/ketahui-6-langkah-penilaian-dan-penanganan-risiko-dalam-iso-27001/. [Accessed 21 Juny 2024].

[19] K. ISO, "Manajemen Risiko Pada ISO 27001:2013," Multiple Training and Consulting, 19 Juny 2024. [Online]. Available: https://konsultaniso.web.id/iso-27001/manajemen-risiko-pada-iso-270012013/. [Accessed 21 Juny 2024].

[20] Hana, "Pentingnya ISO 27001: Atasi Risiko Keamanan Siber Perusahaan Multifinance," Madhava Technology, 30 April 2024. [Online]. Available: https://madhava.id/pentingnya-iso-27001-atasi-risiko-keamanan-siber/. [Accessed 21 Juny 2024].

[21] Admin, "Pengertian Malware serta Jenis dan Cara Mengatasinya Dengan Tepat," Cloudmatika, 15 July 2022. [Online]. Available: https://cloudmatika.co.id/blog-detail/apa-itu-malware. [Accessed 21 Juny 2024].

[22] Administrator, "Mengidentifikasi Dan Mengelola Risiko Dalam Pengadaan Yang Kompleks Pelatihan Pengadaan," Layanan Helpdesk Pemetaan Risiko, 4 September 2020. [Online]. Available: https://helpdesk.inspektorat.babelprov.go.id/berita/detail/mengidentifikasi-dan-mengelola-risiko-dalam-pengadaan-yang-kompleks-pelatihan-pengadaan. [Accessed 24 Juny 2024].

[23] N. L. Athallariq Rafii Nugroho, "Penilaian Risiko di Perusahaan TI dengan Fokus pada Area Keamanan Informasi Menggunakan Iso 27001:2022," *Syntax Literate: Jurnal Ilmiah Indonesia*, vol. VII, no. 12, p. 1, 2022.

LAMPIRAN - LAMPIRAN

Hasil Wawancara Terkait dengan penelitian bersama Pengelola *website official* STT NF yaitu Pak Teguh Prasetyo :

Wawancara Tahap Pertama Untuk Analisis Kebutuhan

Wawancara Seputar SMKI pada Website Official Kampus STT NF

1. Apakah Website STT NF sudah mengimplementasikan standar keamanan SNI ISO/IEC 27001:2022? Tidak
2. Jika belum melaksanakan implementasi standar keamanan tersebut, mengapa? Ketidaktahuan informasi SNI tersebut.
3. Sampai saat ini apa saja kerentanan yang telah dan sering terjadi? Tidak pernah sejak terakhir terkena malware dari sisi server menggunakan keamanan dari provider.
4. Menurut Bapak, mana yang paling tinggi dan mana yang paling rendah diantarakerentanan yang telah terjadi? Serangan Malware
5. Lalu, apakah kerentanan yang disebutkan dapat berdampak tinggi bagi sistem informasi tersebut? Iya, betul. Dapat mengganggu jalannya website stt-nf
6. Apa yang telah dilakukan untuk mengatasi kerentanan tersebut? Melakukan scanning pada level server hingga aplikasi, mendiagnosa permasalahan, dan melakukan perbaikan pada masalah tsb.
7. Bagaimana Untuk mencegah kerentanan tersebut terjadi? Menggunakan keamanan

standar dari CMS, keamanan server, dan maintain update dari CMS tsb

Wawancara Tahap Kedua Untuk Evaluasi

1. Menurut Bapak, apakah penting menerapkan standar keamanan nasional untuk sistem informasi website STT NF untuk mencegah terjadi kembali serangan malware

ataupun serangan lainnya? Tergantung dari sistem yang saat ini digunakan oleh provider. Untuk saat ini sudah cukup menggunakan yang digunakan dari provider.

2. Apakah informasi ini cukup membantu untuk mengetahui sistem keamanan nasional? Cukup membantu.
3. Apakah kerentanan yang telah terjadi bisa saja terulang kembali? Mungkin iya.

Namun sudah dibuat aturan untuk hardening security dari sisi internal dan provider.

4. Apa kekurangan dari hasil asesmen risiko yang telah dilakukan? Spek security server yang ada di pihak tim IT dan provider. Sebagai end-user admin tidak mengetahui bagaimana securitynya.

Bukti Wawancara :