Pengembangan Model Penilaian Kepatuhan Salah Satu Perguruan Tinggi Terhadap Standar ISO 27001:2022

http://dx.doi.org/10.28932/jutisi.v9i3.6850

Riwayat Artikel
Received: 30 Juni 2023 | *Final Revision*: 15 Desember 2023 | *Accepted*: 15 Desember 2023

Rudolf Sinaga✉

Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Dinamika Bangsa
Jalan Jendral Sudirman Thehok - Jambi 36138, Indonesia
rudolf@unama.ac.id
✉Corresponding author: rudolfverdinan@gmail.com

Abstrak — **Sistem keamanan informasi penting bagi organisasi, termasuk perguruan tinggi karena merupakan aspek yang krusial dalam dunia digital saat ini. Dalam konteks ini ISO 27001:2022 adalah standar penting. Salah satu perguruan tinggi yang ada di Kota Jambi mengelola data sensitif , menggunakan berbagai sistem informasi seperti data mahasiswa, dosen, keuangan, pegawai dan penelitian, ini tentu akan meningkatkan kerumitan tata kelola sistem keamanan informasi. Perguruan tinggi juga memiliki komunitas akademik yang terbuka, yang terdiri dari mahasiswa, alumni, dosen, dan staf administrasi, yang memberi peluang meningkatnya risiko keamanan sistem informasi, seperti serangan phishing dan malware. Tujuan penelitian ini adalah untuk mengembangkan model penilaian kepatuhan organisasi perguruan tinggi terhadap standar ISO 27001:2022 dan menerapkan model tersebut pada salah satu perguruan tinggi yang ada di Kota Jambi. Evaluasi menunjukkan bahwa Perguruan Tinggi tersebut memiliki tingkat kepatuhan yang tinggi terhadap keamanan fisik dan lingkungan, tetapi area-area seperti kebijakan keamanan informasi, manajemen risiko, aset informasi, pengendalian akses, keamanan jaringan, serta manajemen insiden keamanan memerlukan peningkatan kepatuhan. Rekomendasi perbaikan dan peningkatan diberikan untuk setiap area yang memerlukan perhatian lebih, sesuai standar ISO 27001:2022 meliputi pengembangan identifikasi risiko, pengelolaan risiko, identifikasi aset informasi yang penting, perlindungan aset informasi, perlindungan terhadap serangan jaringan, pemantauan keamanan jaringan secara teratur, prosedur pengembangan respon kejadian yang efektif, pelaporan kejadian keamanan, dan pembelajaran dari kejadian yang terjadi. Kesimpulannya, pengembangan model penilaian kepatuhan organisasi salah satu perguruan tinggi yang ada di Kota Jambi terhadap standar ISO 27001:2022 memberikan pandangan menyeluruh tentang tingkat kepatuhan pada berbagai area keamanan sistem informasi. Melalui identifikasi kelemahan dan rekomendasi perbaikan yang disusun, langkah-langkah konkret dapat diambil untuk meningkatkan kepatuhan dan mengelola keamanan sistem informasi dengan lebih efektif.**

Kata Kunci: **ISO 27001:2022; keamanan sistem informasi; penilaian tingkat kepatuhan; pengembangan model penilaian.**

Development of a Compliance Assessment Model for One of the Universities to ISO 27001:2022 Standards

Abstract — ***Information security systems are important for organizations, including universities, because they are a crucial aspect of today's digital world. In this context ISO 27001:2022 is an important standard. One of the universities in Jambi City manages sensitive data, using various information systems such as student data, lecturers, finance, employees and research, this will certainly increase***

the complexity of information security system governance. The college also has an open academic community, consisting of students, alumni, faculty, and administrative staff, which provides opportunities for increased information system security risks, such as phishing and malware attacks. This study aims to develop an assessment model for the compliance of higher education organizations with ISO 27001:2022 standards and apply the model to one of the universities in Jambi City. Evaluations show that the universities has a high level of compliance with physical and environmental security, but areas such as information security policy, risk management, information assets, access control, network security, as well as security incident management require increased compliance. Recommendations for improvement and improvement are given for each area that requires more attention, according to the ISO 27001:2022 standard including the development of risk identification, risk management, identification of important information assets, protection of information assets, protection against network attacks, regular network security monitoring, procedures for developing effective event response, reporting of security events, and learning from events that occur. In conclusion, the development of one of the universities in Jambi City organization's compliance assessment model with the ISO 27001:2022 standard provides a comprehensive view of the level of compliance in various areas of information system security. Through the identification of weaknesses and the recommendations for improvement that are drafted, concrete steps can be taken to improve compliance and manage information system security more effectively.

Keywords: ***assessment model development; compliance assessment; ISO 27001:2022; information system security.***

I. PENDAHULUAN

Perguruan tinggi merupakan entitas yang memiliki tanggung jawab besar dalam menjaga keamanan sistem informasi mereka. [1], [2] Dalam era digital yang semakin maju seperti saat ini, perguruan tinggi tidak hanya menghadapi risiko kehilangan data sensitif, tetapi juga serangan siber yang semakin kompleks dan sering kali berdampak luas. [3] Oleh karena itu, menjaga keamanan sistem informasi menjadi hal yang sangat penting bagi perguruan tinggi dalam menjalankan operasi atau kegiatan mereka dengan efektif dan melindungi aset informasi yang berharga. [4]

Setiap perguruan tinggi memiliki karakteristik unik yang berbeda-beda, baik dari segi akademik, komunitas akademik, maupun lingkungannya. Karakteristik unik ini dapat mempengaruhi kebutuhan dan risiko keamanan sistem informasi perguruan tinggi. Oleh karena itu, tata kelola keamanan sistem informasi perguruan tinggi perlu disesuaikan dengan karakteristik unik masing-masing perguruan tinggi. Salah satu perguruan tinggi yang ada di Kota Jambi memiliki karakteristik unik seperti lingkungan TI yang kompleks, termasuk jaringan, sistem basis data, dan aplikasi yang dapat diakses secara luas, hal ini menuntut perguruan tinggi untuk memiliki standar dalam membantu mengelola risiko keamanan. Selain itu Perguruan tinggi tersebut juga menyimpan banyak informasi sensitif tentang mahasiswa, termasuk data pribadi, aktivitas akademik, informasi keuangan, informasi dosen, dan informasi pegawai yang aksesnya terbagi dari beberapa unit sehingga sangat perlu melindungi data tersebut secara efektif dan mematuhi regulasi privasi. [5], [6]

Perguruan tinggi juga bermitra dengan penyedia layanan pihak ketiga, termasuk penyedia layanan cloud. ISO 27001:2022 dapat membantu dalam mengelola risiko keamanan terkait dengan mitra tersebut. Disisi lain Perguruan tinggi juga memiliki risiko khusus dalam lingkungan pendidikan, seperti ancaman terhadap layanan jaringan Wi-Fi publik yang disediakan perguruan tinggi. Selain itu reputasi dan citra merupakan hal yang sangat penting bagi perguruan tinggi ini, maka dengan mematuhi standar ISO 27001:2022, perguruan tinggi akan dapat menunjukkan komitmen terhadap keamanan informasi, yang dapat mempengaruhi citra perguruan tinggi tersebut, baik dari sisi masyarakat maupun dari sisi regulasi.

Dari penjelasan tentang karakteristik unik dan kompleksitas dari keamanan sistem informasi pada perguruan tinggi tersebut, maka memilih penggunaan Standar ISO 27001:2022 menjadi solusi sebuah kerangka kerja untuk menerapkan manajemen keamanan sistem informasi yang lebih baik karena standar ini merupakan standar terbaru dari ISO 27001 yang berbeda dari standar ISO 27001 pendahulunya yang hanya berfokus pada dokumen, sedangkan standar ISO 27001:2022 ini lebih berfokus pada proses, keamanan siber dan privasi yang harus terpadu tidak dipisah seperti pada standar sebelumnya, peningkatan keberlanjutan sangat ditekankan pada standar ini sedangkan pada standar sebelumnya tidak ditekankan. [7]

Standar ISO 27001:2022 sebagai pembaruan standar ISO 27001-2013 telah diterima secara luas sebagai kerangka kerja yang komprehensif dalam mengelola keamanan sistem informasi. [8] Standar ini memberikan pedoman yang jelas dan terstruktur untuk mengidentifikasi, mengevaluasi, dan mengurangi risiko keamanan informasi dalam suatu organisasi. ISO/27001:2022 memiliki beberapa perbedaan dengan versi terdahulunya, yaitu ISO/27001:2005 dan ISO/27001:2013. Beberapa perbedaan tersebut yaitu :

1. Kerangka kerja yang lebih komprehensif: ISO/27001:2022 menyediakan kerangka kerja yang lebih komprehensif untuk menerapkan SMKI. Kerangka kerja ini mencakup aspek-aspek keamanan informasi yang lebih luas, seperti keamanan data, keamanan proses bisnis, dan keamanan lingkungan.
2. Penekanan pada risiko: ISO/27001:2022 menekankan pada penilaian dan pengelolaan risiko keamanan informasi. Standar ini mengharuskan organisasi untuk melakukan penilaian risiko secara berkala untuk mengidentifikasi dan mengurangi risiko keamanan informasi.
3. Kebutuhan untuk mempertimbangkan aspek lingkungan: ISO/27001:2022 mengharuskan organisasi untuk mempertimbangkan aspek lingkungan dalam penerapan SMKI. Hal ini bertujuan untuk memastikan bahwa SMKI tidak menimbulkan dampak negatif terhadap lingkungan.

Berikut adalah beberapa kelebihan ISO/27001:2022:

1. Kerangka kerja yang lebih komprehensif: Kerangka kerja yang lebih komprehensif dapat membantu organisasi untuk meningkatkan keamanan informasi secara keseluruhan.
2. Penekanan pada risiko: Penekanan pada risiko dapat membantu organisasi untuk mengidentifikasi dan mengurangi risiko keamanan informasi secara efektif.
3. Kebutuhan untuk mempertimbangkan aspek lingkungan: Kebutuhan untuk mempertimbangkan aspek lingkungan dapat membantu organisasi untuk menerapkan SMKI yang lebih berkelanjutan.

Kekurangan ISO/27001:2022 yaitu merupakan standar yang kompleks dan membutuhkan pemahaman yang mendalam tentang keamanan informasi.

Berikut adalah beberapa contoh komponen ISO/27001:2022 yang dapat dihadirkan dan diulas dengan baik:

1. Kebijakan keamanan informasi: Kebijakan keamanan informasi adalah dokumen yang menetapkan tujuan dan sasaran keamanan informasi organisasi. Kebijakan ini harus dikomunikasikan kepada seluruh karyawan dan pemangku kepentingan.
2. Penilaian risiko keamanan informasi: Penilaian risiko keamanan informasi adalah proses untuk mengidentifikasi dan mengevaluasi risiko keamanan informasi organisasi. Hasil penilaian risiko ini digunakan untuk menentukan kontrol keamanan seperti apa yang diperlukan.
3. Kontrol keamanan: Kontrol keamanan adalah tindakan yang diambil untuk mengurangi risiko keamanan informasi. Kontrol keamanan dapat berupa teknis, administratif, atau keorganisasian.
4. Pengukuran kinerja SMKI: Pengukuran kinerja SMKI adalah proses untuk mengukur efektivitas penerapan SMKI. Pengukuran kinerja ini dapat dilakukan dengan menggunakan berbagai metode, seperti audit, survei, dan analisis data.
5. Peningkatan SMKI: Peningkatan SMKI adalah proses untuk meningkatkan efektivitas SMKI secara berkelanjutan. Proses ini dapat dilakukan dengan mengidentifikasi peluang untuk perbaikan dan menerapkan perbaikan tersebut. [7]

Namun, implementasi dan penilaian kepatuhan terhadap standar ini di perguruan tinggi masih menjadi tantangan yang kompleks dan unik. Dalam konteks ini, pengembangan model penilaian yang tepat untuk mengevaluasi kepatuhan organisasi perguruan tinggi, seperti salah satu perguruan tinggi yang ada di Kota Jambi, terhadap standar ISO 27001:2022 menjadi sangat penting. [9] Model penilaian ini akan membantu perguruan tinggi dalam mengukur sejauh mana kepatuhan mereka terhadap standar tersebut, mengidentifikasi kelemahan dan celah keamanan yang perlu diperbaiki, serta menyediakan panduan untuk mengambil tindakan perbaikan yang tepat.

Penelitian ini bertujuan untuk mengembangkan model penilaian yang spesifik dan relevan untuk salah satu perguruan tinggi yang ada di Kota Jambi dalam mengevaluasi kepatuhan mereka terhadap standar ISO 27001:2022. Model ini akan dirancang untuk mempertimbangkan kebutuhan dan karakteristik unik dari Salah satu perguruan tinggi yang ada di Kota Jambi serta tantangan yang mereka hadapi dalam mengelola keamanan sistem informasi. Metode yang digunakan dalam penelitian ini meliputi tinjauan literatur tentang standar ISO 27001:2022, praktik dalam pengembangan model penilaian kepatuhan, serta pengumpulan data melalui wawancara dan survei di salah satu perguruan tinggi yang ada di Kota Jambi. Data yang terkumpul akan dianalisis secara sistematis untuk mengidentifikasi persyaratan kepatuhan yang paling relevan dengan lingkungan Salah satu perguruan tinggi yang ada di Kota Jambi serta memahami aspek yang mempengaruhi tingkat kepatuhan.

Penelitian terkait pengembangan model penilaian kepatuhan organisasi terhadap standar ISO telah dilakukan beberapa penulis sebelumnya, diantaranya penelitian pertama yang dilakukan oleh Sigit Tri Yuwono, dkk. Dalam penelitiannya tentang Re-Assessment Konsistensi Dokumen Kontrol Sertifikasi ISO 27001:2013 (SMKI) [10] di Bagian Komunikasi Satelit Monitoring PT. Bank BRI, TBK, untuk menguji kontrol konsistensi pelaksanaan standar selalu sesuai dengan kebijakan yang telah ditetapkan dan pasal ketentuan sertifikasi. Sementara penelitian kedua yang dilakukan oleh Nurkomar Hidaya dan Ihsan Jatnika yang melakukan perancangan Sistem Manajemen Keamanan Informasi Data Center Standart SNI ISO/IEC 27001:2013 untuk memberikan gambaran resiko yang akan terjadi, dampaknya serta langkah pengendalian yang akan diterapkan terhadap resiko keamanan informasi, dengan tujuan akan menghasilkan dokumen yang dapat menjadi pedoman umum dalam penerapan standar ISO 27001:2013 yang selaras dengan kebutuhan perusahaan. [11] Penelitian ketiga yang dilakukan oleh Heri Wahyuni, dkk untuk Mengaudit Keamanan Sistem Informasi Manajemen Akademik dan Kemahasiswaan juga menggunakan SNI ISO-IEC 27001-2013. Penelitian keempat yang dilakukan oleh Hikam Haikal, dkk tentang Perancangan Tata Kelola Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik (SPBE) Menggunakan Standar ISO 27001:2013 dalam rangka melakukan pemetaan tingkat kesenjangan standar terhadap risiko, menganalisis risiko dan membuat prioritas risiko serta memberikan rekomendasi sesuai dengan tingkat risiko terkait. [12] Sementara penelitian lain yang dilakukan Marliana Budhiningtias dan Ismail tentang kerangka kerja Standar ISO 27001:2005 dalam melakukan audit

keamanan sistem informasi akademik perguruan tinggi menghasilkan temuan beberapa kekurangan pada kontrol keamanan seperti peran dan tanggung jawab keamanan, perlindungan fisik dari bencana dan gangguan listrik dan kurangnya validasi data, serta pelaksanaan backup data yang kurang teratur. [13]

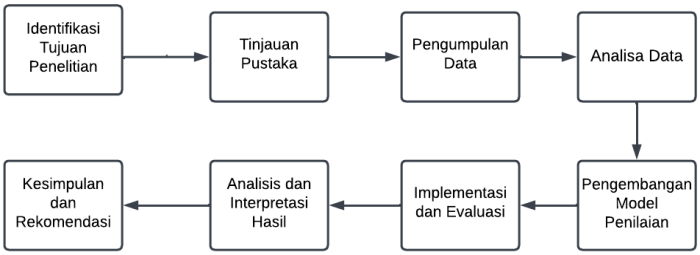
Berdasarkan beberapa penelitian yang dilakukan tersebut, dapat disimpulkan bahwa standar ISO 27001 sangat ideal diterapkan diberbagai bidang organisasi termasuk diantaranya pada lingkungan perguruan tinggi, karena standar ini fokus dalam mengatur manajemen keamanan sistem informasi dan dapat disesuaikan dengan kebutuhan berdasarkan keunikan dari setiap organisasi. [14], [15], [16] Namun penelitian tersebut masih menggunakan standar ISO 27001:2005 dan ISO 27001:2013, sedangkan masalah keamanan sistem informasi saat ini sudah semakin kompleks, sehingga membutuhkan penyesuaian dalam standar keamanan.

Hasil dari penelitian ini diharapkan akan memberikan salah satu perguruan tinggi yang ada di Kota Jambi sebuah model penilaian tingkat kepatuhan yang terstruktur dan komprehensif. Model ini akan membantu salah satu perguruan tinggi yang ada di Kota Jambi dalam mengidentifikasi area kepatuhan yang perlu ditingkatkan, mengukur tingkat kepatuhan saat ini, serta menyediakan pedoman untuk mengambil tindakan perbaikan yang tepat dan efektif. Dalam konteks yang semakin kompleks dan terus berkembang di bidang keamanan sistem informasi, salah satu perguruan tinggi yang ada di Kota Jambi harus mampu menghadapi ancaman yang semakin besar dan menjaga kepercayaan sivitas akademika serta stakeholders. Dengan menggunakan model penilaian yang sesuai, salah satu perguruan tinggi yang ada di Kota Jambi akan dapat memperkuat sistem keamanan mereka, melindungi aset informasi yang sensitif, dan memastikan kepatuhan terhadap standar ISO 27001:2022 dalam mengelola keamanan sistem informasi.

II. METODE PENELITIAN

A. Tahapan Penelitian

Untuk merencanakan langkah-langkah yang tepat untuk menjawab pertanyaan penelitian maka perlu dibuat sebuah metodologi penelitian, berikut adalah tahapan penelitian yang dilakukan dapat dilihat pada gambar 1:



Gambar 1. Diagram Alir Penelitian

Pada gambar 1 diagram alir penelitian akan dijelaskan sebagai berikut:

1) Identifikasi Tujuan Penelitian:
   Pada tahapan ini dilakukan penentuan tujuan penelitian secara jelas yaitu untuk mengembangkan model penilaian kepatuhan, mengidentifikasi kesenjangan kepatuhan, atau mengevaluasi tingkat kepatuhan organisasi Salah satu perguruan tinggi yang ada di Kota Jambi terhadap standar ISO 27001:2022.
2) Tinjauan Pustaka:
   Pada tahapan ini dilakukan studi literatur yang komprehensif tentang kepatuhan terhadap standar ISO 27001:2022, pengelolaan keamanan sistem informasi di perguruan tinggi, dan metode penilaian kepatuhan yang telah diterapkan sebelumnya. Identifikasi kerangka kerja dan model yang relevan yang dapat menjadi dasar untuk pengembangan model penilaian.
3) Pengumpulan Data:
   Tahapan ini merupakan aktivitas yang dilakukan dalam mengidentifikasi sumber data yang diperlukan, seperti kebijakan dan prosedur keamanan, laporan audit sebelumnya, dokumentasi keamanan, dan data terkait lainnya. Pengumpulan data dilakukan dengan menggunakan metode-metode seperti wawancara, survei, observasi, atau analisis dokumen.
4) Analisis Data:
   Setelah dilakukan proses pengumpulan data maka selanjutnya dilakukan analisis data yang telah dikumpulkan untuk mengidentifikasi indikator kepatuhan yang relevan dengan standar ISO 27001:2022 dan menjadi landasan untuk membuat kriteria penilaian yang jelas dan terukur untuk mengevaluasi tingkat kepatuhan Salah satu perguruan tinggi yang ada di Kota Jambi.

5) Pengembangan Model Penilaian:
Selanjutnya hasil analisis data dan temuan penelitian sebelumnya digunakan untuk mengembangkan model penilaian kepatuhan. Dimana model ini harus mencakup komponen evaluasi yang relevan dengan persyaratan standar ISO 27001:2022 dan dapat memberikan tingkat kepatuhan yang objektif dan terukur.
6) Implementasi dan Evaluasi:
Tahapan berikutnya adalah mengimplementasikan model penilaian pada organisasi salah satu perguruan tinggi yang ada di Kota Jambi dan mengumpulkan data untuk mengevaluasi tingkat kepatuhan mereka terhadap standar ISO 27001:2022.
7) Analisis dan Interpretasi Hasil:
Selanjutnya akan dilakukan analisis hasil evaluasi kemudian menginterpretasikan data yang terkumpul. Dari hasi tersebut akan dilakukan proses identifikasi kekuatan, kelemahan, dan area perbaikan yang terkait dengan kepatuhan organisasi Salah satu perguruan tinggi yang ada di Kota Jambi terhadap standar ISO 27001:2022.
8) Kesimpulan dan Rekomendasi:
Tahapan berikutnya adalah membuat kesimpulan tentang tingkat kepatuhan organisasi salah satu perguruan tinggi yang ada di Kota Jambi terhadap standar ISO 27001:2022, serta memberikan rekomendasi untuk perbaikan dan pengembangan kebijakan dan praktik keamanan sistem informasi yang lebih baik.

B. Standar ISO 27001:2022

Standar ISO 27001:2022 adalah standar internasional yang diterbitkan oleh *International Organization for Standardization* (ISO) yang mengatur sistem manajemen keamanan informasi (*Information Security Management System*/SMKI). Standar ini memberikan kerangka kerja yang komprehensif bagi organisasi dalam mengelola keamanan informasi dengan efektif. Standar ini resmi dipublikasi pada bulan Oktober 2022, meskipun standar pendahulunya yaitu ISO 27001-2013 saat ini masih dapat digunakan selama masa transisi hingga Oktober 2025, namun organisasi harus sudah mulai beradaptasi dengan standar yang baru ini, sebab adanya perbaikan dari standar sebelumnya. [8]

ISO 27001:2022 berfokus pada perlindungan informasi yang penting bagi organisasi, termasuk data sensitif, informasi pelanggan, informasi keuangan, dan informasi lainnya yang memiliki nilai penting. Standar ini dirancang untuk membantu organisasi dalam membangun, menerapkan, mengoperasikan, memantau, memelihara, dan meningkatkan sistem manajemen keamanan informasi mereka. ISO 27001:2022 menyediakan kerangka kerja yang holistik dan sistematis untuk mengelola risiko keamanan informasi. Standar ini mencakup berbagai aspek keamanan informasi, termasuk kebijakan keamanan informasi, identifikasi aset informasi, analisis risiko, pengendalian keamanan informasi, manajemen insiden keamanan, dan tinjauan berkelanjutan.

Adapun persyaratan, kebijakan, prosedur, dan praktik terkait keamanan sistem informasi yang tercakup dalam standar ISO 27001:2022:

1) Persyaratan Keamanan Informasi: menetapkan kebijakan keamanan informasi yang relevan dengan tujuan dan konteks organisasi, melakukan analisis risiko untuk mengidentifikasi ancaman, kerentanan, dan dampak yang mungkin terjadi pada aset informasi, mengembangkan dan menerapkan pengendalian keamanan informasi yang sesuai untuk mengurangi risiko yang teridentifikasi, melakukan pemantauan, pengukuran, analisis, dan evaluasi secara teratur terhadap keefektifan pengendalian keamanan informasi yang ada, melakukan pemutakhiran dan perbaikan berkelanjutan pada sistem manajemen keamanan informasi.
2) Kebijakan Keamanan Informasi: menetapkan kebijakan keamanan informasi yang jelas, yang mencakup tanggung jawab dan komitmen dari pimpinan organisasi, menyampaikan kebijakan keamanan informasi secara efektif kepada seluruh anggota organisasi dan pihak terkait, memastikan bahwa kebijakan keamanan informasi diperbarui secara berkala sesuai dengan perkembangan organisasi dan lingkungan bisnis.
3) Prosedur Keamanan Informasi: mengembangkan prosedur yang terdokumentasi untuk mengelola aset informasi, termasuk pengelolaan akses, pengendalian perubahan, pemantauan, dan respons terhadap insiden keamanan, menetapkan prosedur untuk melibatkan pihak terkait dalam pengelolaan keamanan informasi, seperti pemasok, mitra bisnis, dan pengguna akhir, memastikan bahwa prosedur keamanan informasi dijalankan secara konsisten dan diawasi secara berkala untuk memastikan kepatuhan terhadap kebijakan dan standar yang ditetapkan.
4) Praktik Keamanan Informasi: mengelola akses fisik ke area yang mengandung aset informasi penting, seperti ruang server atau pusat data, mengimplementasikan kebijakan keamanan yang ketat terkait dengan penggunaan dan pengelolaan kata sandi, melakukan pemantauan jaringan dan sistem untuk mendeteksi aktivitas yang mencurigakan atau serangan potensial, mengamankan komunikasi dan transmisi data melalui enkripsi dan teknologi keamanan yang sesuai, melakukan pengujian keamanan secara berkala untuk mengidentifikasi kerentanan dan memastikan kepatuhan terhadap kebijakan dan prosedur yang ditetapkan.

Dengan mengadopsi standar ISO 27001:2022, organisasi dapat mengidentifikasi, mengelola, dan memitigasi risiko keamanan informasi dengan cara yang sistematis dan terstruktur. Standar ini juga membantu organisasi dalam membangun budaya keamanan yang kuat, meningkatkan kesadaran keamanan, dan memastikan kepatuhan terhadap persyaratan hukum, peraturan, dan kontrak yang berlaku. ISO 27001:2022 berlaku secara universal dan dapat diimplementasikan oleh organisasi dari berbagai sektor dan ukuran. Standar ini memberikan kerangka kerja yang fleksibel sehingga dapat disesuaikan dengan kebutuhan unik setiap organisasi. Dengan menerapkan standar ini, organisasi dapat meningkatkan kepercayaan pelanggan, memitigasi risiko keamanan informasi, dan meningkatkan daya saing di pasar. ISO 27001:2022 adalah revisi terbaru dari standar ISO 27001, yang menggantikan versi sebelumnya, yaitu ISO 27001-2013. Perbedaan antara kedua versi tersebut meliputi perubahan dalam konteks, struktur, dan persyaratan yang terkait dengan manajemen keamanan informasi. Berikut adalah beberapa perbedaan utama antara ISO 27001:2022 dan ISO 27001-2013:

1) Konteks yang Lebih Relevan:
   ISO 27001:2022 mengadopsi pendekatan yang lebih kontekstual dalam mengelola keamanan informasi. Standar ini menekankan pentingnya memahami konteks organisasi, termasuk faktor internal dan eksternal yang mempengaruhi keamanan informasi. Hal ini membantu organisasi dalam menyesuaikan pendekatan keamanan informasi dengan tujuan, risiko, dan kebutuhan mereka.
2) Penekanan pada Risiko:
   ISO 27001:2022 menempatkan lebih banyak penekanan pada analisis risiko dan perlindungan terhadap risiko keamanan informasi. Standar ini mendorong organisasi untuk mengidentifikasi, menilai, dan mengelola risiko yang relevan dengan aset informasi mereka dengan lebih efektif.
3) Struktur yang Diperbarui:
   ISO 27001:2022 mengadopsi struktur yang sejalan dengan kerangka kerja manajemen risiko ISO 31000. Standar ini mengikuti struktur kerangka kerja manajemen risiko yang dikenal sebagai "*High-Level Structure*" (HLS), yang memudahkan integrasi dengan standar ISO lainnya.
4) Penyederhanaan Persyaratan:
   ISO 27001:2022 mengurangi beberapa persyaratan yang dianggap ambigu dalam versi sebelumnya. Hal ini bertujuan untuk membuat standar lebih jelas dan lebih mudah dipahami oleh organisasi yang menerapkannya.
5) Peningkatan Kepatuhan:
   ISO 27001:2022 memperkuat persyaratan terkait kepatuhan hukum, peraturan, dan kontrak yang berlaku. Standar ini mendorong organisasi untuk memastikan kepatuhan terhadap persyaratan yang relevan dan memperkuat sistem manajemen keamanan informasi mereka.

Selain perbedaan tersebut, ISO 27001:2022 juga mencakup pembaruan dan adanya peningkatan lainnya untuk tetap menjaga relevansi dan keefektifan standar dalam menghadapi perkembangan teknologi dan ancaman keamanan informasi yang terus berubah.

III. HASIL DAN PEMBAHASAN

A. Identifikasi Kebutuhan Perguruan Tinggi

Perguruan tinggi menghadapi tantangan unik dalam mengelola keamanan sistem informasi karena lingkungan mereka yang kompleks dan beragam, demikian halnya pada salah satu perguruan tinggi yang ada di Kota Jambi. Berdasarkan hasil observasi dan wawancara yang dilakukan, berikut adalah beberapa kebutuhan, tujuan, dan tantangan spesifik yang dihadapi oleh perguruan tinggi tersebut dalam mengelola keamanan sistem informasi:

1) Kebutuhan Privasi dan Perlindungan Data: Perguruan tinggi tersebut seringkali mengelola jumlah besar data sensitif, termasuk informasi pribadi mahasiswa, data penelitian mahasiswa, data portofolio dosen dan informasi administratif. Mereka harus memastikan perlindungan data yang memadai dan kepatuhan terhadap regulasi privasi yang berlaku, seperti Undang-undang No. 27 tahun 2022 tentang perlindungan data pribadi. [17]
2) Ketergantungan pada Sistem Informasi: Sesuai dengan tuntutan layanan perguruan tinggi yang prima, Perguruan tinggi tersebut mengandalkan sistem informasi untuk berbagai kegiatan, termasuk pengelolaan administrasi, kegiatan tridharma dosen, kegiatan akademik, dan layanan mahasiswa. Oleh karena itu ketersediaan, integritas, dan kerahasiaan sistem informasi harus dijaga dengan baik untuk memastikan kelancaran operasional kampus.
3) Akses Terhadap Informasi: Perguruan tinggi tersebut memiliki berbagai pemangku kepentingan, termasuk mahasiswa, dosen, staf, biro akademik, dan mitra eksternal. Maka harus memastikan akses yang sesuai dan terkelola dengan baik terhadap informasi yang relevan adalah penting untuk mendukung fungsi akademik, tridharma, dan administrasi.
4) Kebutuhan Keberlanjutan: Perguruan tinggi tersebut beroperasi dalam jangka waktu yang panjang dan harus mampu menjaga keamanan sistem informasi secara berkelanjutan. Hal ini melibatkan seperti pembaruan rutin, pemantauan keamanan, dan respons terhadap ancaman yang berkembang.

5) Tantangan Teknis: Lingkungan IT di perguruan tinggi tersebut sudah termasuk kompleks dengan infrastruktur yang beragam, termasuk sistem yang dihosting secara internal maupun di *cloud*, dan jaringan nirkabel. Tentu untuk mengelola keamanan sistem informasi dalam lingkungan yang kompleks ini membutuhkan pemahaman yang mendalam tentang kerentanan dan ancaman yang mungkin timbul.
6) Kesadaran dan Pelatihan: Perlunya meningkatkan tingkat kesadaran tentang keamanan informasi di kalangan mahasiswa, dosen, dan staf menjadi faktor penting dalam menjaga keamanan sistem informasi. Perguruan tinggi tersebut perlu menyelenggarakan pelatihan dan mengedukasi pemangku kepentingan tentang praktik keamanan yang baik dan pentingnya kepatuhan terhadap kebijakan keamanan.
7) Keterbatasan Sumber Daya: Perguruan tinggi tersebut menghadapi keterbatasan sumber daya manusia, keuangan, dan infrastruktur. Sehingga mengelola keamanan sistem informasi dengan sumber daya yang terbatas ini dapat menjadi tantangan, dan perlu dilakukan alokasi yang cerdas dan prioritas yang jelas dalam mengatasi risiko keamanan.

B. Penentuan Indikator Kepatuhan

Berdasarkan hasil identifikasi kebutuhan perguruan tinggi, beberapa indikator kepatuhan yang relevan dengan standar ISO 27001:2022 yang dapat diukur dan dinilai secara objektif dalam konteks Perguruan Tinggi tersebut:

1) Kebijakan Keamanan Informasi: Persyaratan untuk memiliki kebijakan keamanan informasi yang ditetapkan, disetujui, dan dikomunikasikan kepada seluruh pemangku kepentingan. Indikator kepatuhan mencakup:
    a. Persentase kebijakan keamanan informasi yang telah ditetapkan dan disetujui.
    b. Tingkat pemahaman dan kesadaran pemangku kepentingan terhadap kebijakan keamanan informasi.
2) Manajemen Risiko: Persyaratan untuk melakukan identifikasi, penilaian, dan penanganan risiko terkait keamanan informasi. Indikator kepatuhan mencakup:
    a. Jumlah risiko yang diidentifikasi dan dinilai.
    b. Tingkat penanganan risiko yang dilakukan (seperti, jumlah risiko yang telah dihilangkan atau dikurangi).
3) Aset Informasi: Persyaratan untuk mengidentifikasi dan melindungi aset informasi yang penting. Indikator kepatuhan dapat mencakup:
    a. Daftar aset informasi yang penting dan perlindungan yang diterapkan.
    b. Tingkat kepatuhan terhadap kebijakan dan prosedur perlindungan aset informasi.
4) Keamanan Fisik dan Lingkungan: Persyaratan untuk melindungi fasilitas fisik dan lingkungan tempat aset informasi disimpan. Indikator kepatuhan mencakup:
    a. Penerapan langkah-langkah keamanan fisik, seperti penguncian, pengawasan, dan pengendalian akses.
    b. Tingkat kepatuhan terhadap prosedur keamanan saat mengakses ruang fisik yang berisi aset informasi.
5) Pengendalian Akses: Persyaratan untuk memastikan akses yang tepat dan terbatas ke aset informasi. Indikator kepatuhan mencakup:
    a. Tingkat implementasi mekanisme otentikasi (misalnya, *username* dan *password*) untuk mengontrol akses.
    b. Tingkat pemantauan dan pengendalian terhadap hak akses yang diberikan kepada pengguna.
6) Keamanan Jaringan dan Komunikasi: Persyaratan untuk melindungi jaringan dan komunikasi dari ancaman dan serangan. Indikator kepatuhan mencakup:
    a. Implementasi kebijakan dan kontrol keamanan jaringan, seperti firewall dan enkripsi data.
    b. Tingkat kepatuhan terhadap prosedur dan kebijakan keamanan saat menggunakan komunikasi elektronik.
7) Manajemen Insiden Keamanan: Persyaratan untuk merespons dan menangani insiden keamanan informasi. Indikator kepatuhan mencakup:
    a. Waktu respons terhadap insiden keamanan.
    b. Tingkat pemahaman dan kesadaran pemangku kepentingan tentang prosedur penanganan insiden.

C. Pengembangan Kriteria Model Penilaian

Setelah penentuan indikator kepatuhan, berikutnya adalah mengembangkan kriteria model penilaian yang digunakan untuk mengevaluasi tingkat kepatuhan salah satu perguruan tinggi yang ada di Kota Jambi terhadap setiap indikator kepatuhan yang telah disebutkan sebelumnya:

1) Kebijakan Keamanan Informasi:
    a. Jelas dan terdokumentasi: Apakah kebijakan keamanan informasi ditetapkan secara jelas dan didokumentasikan dengan lengkap?
    b. Disetujui dan dikomunikasikan: Apakah kebijakan keamanan informasi telah disetujui oleh pimpinan perguruan tinggi dan dikomunikasikan secara efektif kepada semua pemangku kepentingan?
2) Manajemen Risiko:

a. Identifikasi risiko: Sejauh mana perguruan tinggi telah mengidentifikasi risiko yang terkait dengan keamanan informasi?
b. Penilaian risiko: Sejauh mana perguruan tinggi telah melakukan penilaian risiko secara komprehensif dan menyeluruh?
c. Penanganan risiko: Sejauh mana perguruan tinggi telah menerapkan langkah-langkah yang tepat untuk mengurangi atau menghilangkan risiko yang diidentifikasi?

3) Aset Informasi:
   a. Identifikasi aset: Sejauh mana perguruan tinggi telah mengidentifikasi aset informasi yang penting dan berharga?
   b. Perlindungan aset: Sejauh mana perguruan tinggi telah menerapkan langkah-langkah perlindungan yang memadai untuk aset informasi tersebut?
4) Keamanan Fisik dan Lingkungan:
   a. Pengamanan fasilitas: Sejauh mana perguruan tinggi telah menerapkan langkah-langkah pengamanan fisik di fasilitas penyimpanan aset informasi?
   b. Pengendalian akses fisik: Sejauh mana perguruan tinggi telah menerapkan kontrol akses fisik yang memadai untuk memastikan hanya orang yang berwenang yang dapat mengakses aset informasi?
5) Pengendalian Akses:
   a. Pengelolaan hak akses: Sejauh mana perguruan tinggi telah mengelola hak akses pengguna dengan tepat dan membatasi akses yang tidak perlu?
   b. Mekanisme otentikasi: Sejauh mana perguruan tinggi telah menerapkan mekanisme otentikasi yang kuat dan memadai untuk mengontrol akses pengguna?
6) Keamanan Jaringan dan Komunikasi:
   a. Keamanan jaringan: Sejauh mana perguruan tinggi telah menerapkan kebijakan dan kontrol keamanan yang sesuai untuk melindungi jaringan dari ancaman dan serangan?
   b. Enkripsi komunikasi: Sejauh mana perguruan tinggi telah menerapkan enkripsi yang memadai untuk melindungi komunikasi elektronik?
7) Manajemen Insiden Keamanan:
   a. Respons insiden: Sejauh mana perguruan tinggi memiliki prosedur yang jelas dan responsif untuk menangani insiden keamanan informasi?
   b. Pelaporan insiden: Sejauh mana perguruan tinggi menerapkan pelaporan insiden keamanan secara efektif?

D. Pengumpulan Data

Selanjutnya untuk melakukan penilaian kepatuhan, maka dilakukan pengumpulan data melalui pengisian kuesioner. Dimana data ini mencakup kebijakan, dokumen prosedur, catatan pelatihan, laporan keamanan, dan informasi lain yang berkaitan dengan keamanan sistem informasi di salah satu perguruan tinggi yang ada di Kota Jambi. Berikut daftar pernyataan survey dalam bentuk kuesioner, dapat dilihat pada Tabel 1:

TABEL 1.
DAFTAR PERNYATAAN KUESIONER

No.	Pernyataan	Sangat Tidak Setuju	Tidak Setuju	Netral	Setuju	Sangat Setuju
1	Perguruan Tinggi telah menetapkan kebijakan keamanan informasi yang mencakup aspek ISO 27001:2022					
2	Perguruan Tinggi memiliki tim atau personel yang bertanggung jawab untuk mengelola keamanan sistem informasi secara khusus.					
3	Perguruan Tinggi memiliki prosedur untuk mengidentifikasi dan mengevaluasi risiko keamanan sistem informasi.					
4	Perguruan Tinggi memiliki mekanisme untuk melaksanakan pengendalian keamanan yang relevan dengan ISO 27001:2022.					
5	Perguruan Tinggi secara rutin melakukan audit keamanan sistem informasi untuk memastikan kepatuhan terhadap ISO 27001:2022.					
6	Perguruan Tinggi memiliki kebijakan dan prosedur yang jelas untuk mengelola akses dan penggunaan data sensitif.					
7	Perguruan Tinggi memiliki kebijakan untuk melindungi informasi rahasia dan rahasia dagang yang dimiliki oleh pihak ketiga.					

No.	Pernyataan	Sangat Tidak Setuju	Tidak Setuju	Netral	Setuju	Sangat Setuju
8	Perguruan Tinggi memiliki prosedur untuk melaporkan dan menangani insiden keamanan yang terjadi pada sistem informasi.					
9	Perguruan Tinggi memiliki langkah-langkah untuk memastikan keamanan fisik terhadap akses yang tidak sah ke fasilitasnya.					
10	Perguruan Tinggi memiliki kebijakan untuk melibatkan para pengguna dalam kesadaran keamanan informasi dan pelatihan terkait.					
11	Perguruan Tinggi memiliki prosedur untuk mengelola patch dan pembaruan keamanan sistem operasi dan perangkat lunak.					
12	Perguruan Tinggi memiliki kebijakan dan prosedur untuk menjaga keamanan saat mengoperasikan sistem informasi secara jarak jauh.					
13	Perguruan Tinggi memiliki prosedur untuk memantau dan mendeteksi ancaman keamanan seperti serangan malware atau intrusi.					
14	Perguruan Tinggi memiliki kebijakan dan prosedur yang jelas untuk mengelola penghentian akses dan penghapusan data.					
15	Perguruan Tinggi secara rutin melakukan evaluasi kepatuhan terhadap kebijakan keamanan informasi yang telah ditetapkan.					
16	Perguruan Tinggi meninjau dan memperbarui kebijakan dan prosedur keamanan informasi sesuai dengan perkembangan teknologi dan ancaman keamanan yang terkini					
17	Perguruan Tinggi secara rutin melakukan evaluasi kepatuhan terhadap kebijakan keamanan informasi yang telah ditetapkan.					

E. Analisis Data

Data yang telah dikumpulkan kemudian dianalisis untuk menentukan tingkat kepatuhan Perguruan Tinggi tersebut terhadap indikator kepatuhan yang telah ditentukan. Untuk mengorganisir dan menganalisis data survey, maka digunakan fungsi dan formula spreadsheet untuk menghitung skor kepatuhan, menghasilkan grafik, dan melakukan analisis deskriptif, seperti yang ditampilkan pada Tabel 2 dan Tabel 3 berikut:

TABEL 2.
HASIL PENGISIAN KUESIONER

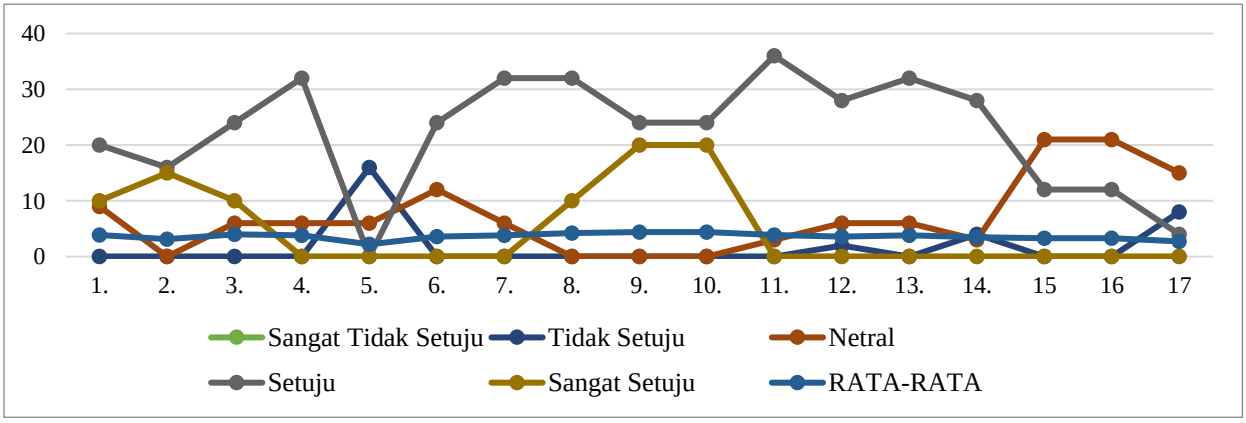
No.	Pertanyaan Survei	Sangat Tidak Setuju	Tidak Setuju	Netral	Setuju	Sangat Setuju
1.	Perguruan Tinggi telah menetapkan kebijakan keamanan informasi yang mencakup aspek ISO 27001:2022.			3	5	2
2.	Perguruan Tinggi memiliki tim atau personel yang bertanggung jawab untuk mengelola keamanan sistem informasi secara khusus.				4	3
3.	Perguruan Tinggi memiliki prosedur untuk mengidentifikasi dan mengevaluasi risiko keamanan sistem informasi.			2	6	2
4.	Perguruan Tinggi memiliki mekanisme untuk melaksanakan pengendalian keamanan yang relevan dengan ISO 27001:2022.			2	8	
5.	Perguruan Tinggi secara rutin melakukan audit keamanan sistem informasi untuk memastikan kepatuhan terhadap ISO 27001:2022.		8	2		
6.	Perguruan Tinggi memiliki kebijakan dan prosedur yang jelas untuk mengelola akses dan penggunaan data sensitif.			4	6	
7.	Perguruan Tinggi memiliki kebijakan untuk melindungi informasi rahasia yang dimiliki oleh pihak ketiga.			2	8	
8.	Perguruan Tinggi memiliki prosedur untuk melaporkan dan menangani insiden keamanan yang terjadi pada sistem informasi.				8	2

No.	Pertanyaan Survei	Sangat Tidak Setuju	Tidak Setuju	Netral	Setuju	Sangat Setuju
9.	Perguruan Tinggi memiliki langkah-langkah untuk memastikan keamanan fisik terhadap akses yang tidak sah ke fasilitasnya.				6	4
10.	Perguruan Tinggi memiliki kebijakan untuk melibatkan para pengguna dalam kesadaran keamanan informasi dan pelatihan terkait.				6	4
11.	Perguruan Tinggi memiliki prosedur untuk mengelola patch dan pembaruan keamanan sistem operasi dan perangkat lunak.			1	9	
12.	Perguruan Tinggi memiliki kebijakan dan prosedur untuk menjaga keamanan saat mengoperasikan sistem informasi secara jarak jauh.		1	2	7	
13.	Perguruan Tinggi memiliki prosedur untuk memantau dan mendeteksi ancaman keamanan seperti serangan malware atau intrusi.			2	8	
14.	Perguruan Tinggi memiliki kebijakan dan prosedur yang jelas untuk mengelola penghentian akses dan penghapusan data.		2	1	7	
15.	Perguruan Tinggi mengelola perubahan dalam kebijakan dan persyaratan kepatuhan yang ditetapkan, serta menyusun rencana tindak lanjut untuk mencapai tingkat kepatuhan yang lebih baik			7	3	
16.	Perguruan Tinggi meninjau dan memperbarui kebijakan dan prosedur keamanan informasi sesuai dengan perkembangan teknologi dan ancaman keamanan yang terkini			7	3	
17.	Perguruan Tinggi secara rutin melakukan evaluasi kepatuhan terhadap kebijakan keamanan informasi yang telah ditetapkan.		4	5	1	

TABEL 3.
HASIL PENGHITUNGAN SKOR KEPATUHAN

No.	Pertanyaan Survei	Sangat Tidak Setuju	Tidak Setuju	Netral	Setuju	Sangat Setuju	Rata-Rata
1.	Perguruan Tinggi telah menetapkan kebijakan keamanan informasi yang mencakup aspek ISO 27001:2022.	0	0	9	20	10	**3,90**
2.	Perguruan Tinggi memiliki tim atau personel yang bertanggung jawab untuk mengelola keamanan sistem informasi secara khusus.	0	0	0	16	15	**3,10**
3.	Perguruan Tinggi memiliki prosedur untuk mengidentifikasi dan mengevaluasi risiko keamanan sistem informasi.	0	0	6	24	10	**4,00**
4.	Perguruan Tinggi memiliki mekanisme untuk melaksanakan pengendalian keamanan yang relevan dengan ISO 27001:2022.	0	0	6	32	0	**3,80**
5.	Perguruan Tinggi secara rutin melakukan audit keamanan sistem informasi untuk memastikan kepatuhan terhadap ISO 27001:2022.	0	16	6	0	0	**2,20**
6.	Perguruan Tinggi memiliki kebijakan dan prosedur yang jelas untuk mengelola akses dan penggunaan data sensitif.	0	0	12	24	0	**3,60**
7.	Perguruan Tinggi memiliki kebijakan untuk melindungi informasi rahasia yang dimiliki oleh pihak ketiga.	0	0	6	32	0	**3,80**
8.	Perguruan Tinggi memiliki prosedur untuk melaporkan dan menangani insiden keamanan yang terjadi pada sistem informasi.	0	0	0	32	10	**4,20**

No.	Pertanyaan Survei	Sangat Tidak Setuju	Tidak Setuju	Netral	Setuju	Sangat Setuju	Rata-Rata
9.	Perguruan Tinggi memiliki langkah-langkah untuk memastikan keamanan fisik terhadap akses yang tidak sah ke fasilitasnya.	0	0	0	24	20	**4,40**
10.	Perguruan Tinggi memiliki kebijakan untuk melibatkan para pengguna dalam kesadaran keamanan informasi dan pelatihan terkait.	0	0	0	24	20	**4,40**
11.	Perguruan Tinggi memiliki prosedur untuk mengelola patch dan pembaruan keamanan sistem operasi dan perangkat lunak.	0	0	3	36	0	**3,90**
12.	Perguruan Tinggi memiliki kebijakan dan prosedur untuk menjaga keamanan saat mengoperasikan sistem informasi secara jarak jauh.	0	2	6	28	0	**3,60**
13.	Perguruan Tinggi memiliki prosedur untuk memantau dan mendeteksi ancaman keamanan seperti serangan malware atau intrusi.	0	0	6	32	0	**3,80**
14.	Perguruan Tinggi memiliki kebijakan dan prosedur yang jelas untuk mengelola penghentian akses dan penghapusan data.	0	4	3	28	0	**3,50**
15.	Perguruan Tinggi mengelola perubahan dalam kebijakan dan persyaratan kepatuhan yang ditetapkan, serta menyusun rencana tindak lanjut untuk mencapai tingkat kepatuhan yang lebih baik	0	0	21	12	0	**3,30**
16.	Perguruan Tinggi meninjau dan memperbarui kebijakan dan prosedur keamanan informasi sesuai dengan perkembangan teknologi dan ancaman keamanan yang terkini	0	0	21	12	0	**3,30**
17.	Perguruan Tinggi secara rutin melakukan evaluasi kepatuhan terhadap kebijakan keamanan informasi yang telah ditetapkan.	0	8	15	4	0	**2,70**

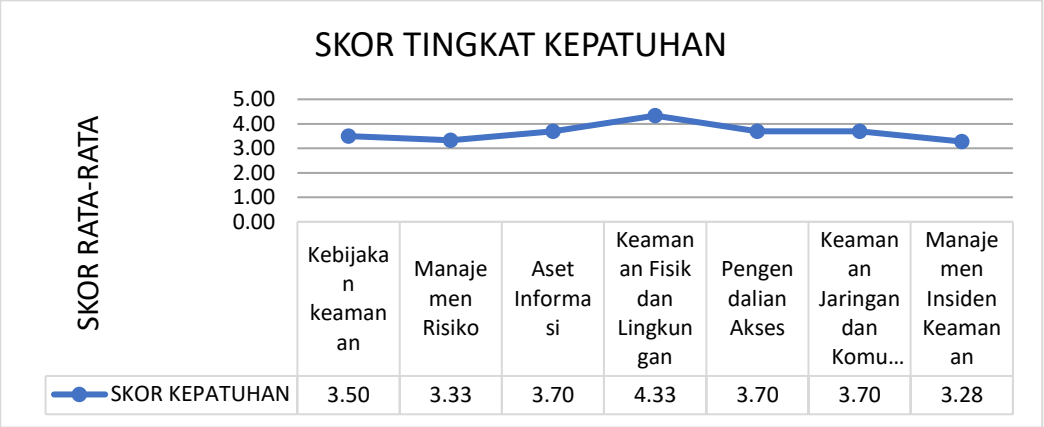


Gambar 2. Hasil Penghitungan Skor Kepatuhan

Dari gambar 2 dapat dilihat hasil penghitungan skor kepatuhan salah satu perguruan tinggi yang ada di Kota Jambi terhadap standar ISO 27001:2022 berdasarkan pengembangan kriteria model penilaian dimasing-masing indikator.

F. Evaluasi Tingkat Kepatuhan

Evaluasi tingkat kepatuhan salah satu perguruan tinggi yang ada di Kota Jambi terhadap standar ISO 27001:2022 berdasarkan hasil analisis data akan dilakukan berdasarkan data seperti pada Gambar 2, kemudian dilanjutkan mengidentifikasi area di mana perguruan tinggi telah mencapai kepatuhan penuh, area yang perlu perbaikan, dan area yang memerlukan tindakan segera.



	Kebijakan keamanan	Manajemen Risiko	Aset Informasi	Keamanan Fisik dan Lingkungan	Pengendalian Akses	Keamanan Jaringan dan Komu...	Manajemen Insiden Keamanan
SKOR KEPATUHAN	3.50	3.33	3.70	4.33	3.70	3.70	3.28

Gambar 3. Skor Rata-Rata Tingkat Kepatuhan

Dari Gambar 3 dapat dijelaskan hasil evaluasi tingkat kepatuhan salah satu perguruan tinggi yang ada di Kota Jambi terhadap setiap indikator yang telah ditentukan sebelumnya, skor rata-rata yang tinggi (di atas 4) menunjukkan tingkat kepatuhan yang lebih tinggi terhadap standar ISO 27001:2022. Pada saat yang sama, skor rata-rata yang rendah (di bawah 3.5) menandakan adanya kekurangan atau ketidakpatuhan terhadap standar tersebut:

1) Kebijakan Keamanan Informasi:
   Berdasarkan indikator kebijakan keamanan informasi dari pernyataan nomor 1 dan 2 dengan skor masing-masing 3,10 dan 3,90 memiliki skor rata-rata 3,50 (sedang)
2) Manajemen Risiko:
   Berdasarkan indikator manajemen risiko dari pernyataan nomor 3, 4 dan 5 dengan skor masing-masing 4,00; 3,80 dan 2,20 memiliki skor rata-rata 3,33 (rendah)
3) Aset Informasi:
   Berdasarkan indikator aset informasi dari pernyataan nomor 6 dan 7 dengan skor masing-masing 3,60 dan 3,80 memiliki skor rata-rata 3,70 (sedang)
4) Keamanan Fisik dan Lingkungan:
   Berdasarkan indikator keamanan fisik dan lingkungan dari pernyataan nomor 8, 9 dan 10 dengan skor masing-masing 4,20; 4,20 dan 4,40 memiliki skor rata-rata 4,33 (tinggi)
5) Pengendalian Akses:
   Berdasarkan indikator pengendalian akses dari pernyataan nomor 11 dan 14 dengan skor masing-masing 3,90 dan 3,50 memiliki skor rata-rata 3,70 (sedang)
6) Keamanan Jaringan dan Komunikasi:
   Berdasarkan indikator keamanan jaringan dan komunikasi dari pernyataan nomor 12 dan 13 dengan skor masing-masing 3,60 dan 3,80 memiliki skor rata-rata 3,70 (sedang)
7) Manajemen Insiden Keamanan:
   Berdasarkan indikator keamanan jaringan dan komunikasi dari pernyataan nomor 15, 16 dan 17 dengan skor masing-masing 3,30; 3,30 dan 2,70 memiliki skor rata-rata 3,28 (rendah)

Dari hasil evaluasi dilanjutkan proses Identifikasi Prioritas Kepatuhan. Identifikasi berdasarkan indikator yang mendapatkan skor rata-rata rendah atau di bawah ambang batas yang telah ditetapkan sebelumnya adalah pada area Manajemen Risiko dan Manajemen Insiden Keamanan, sementara area Kebijakan Keamanan Informasi, Aset Informasi,

Pengendalian Akses, serta Keamanan Jaringan dan Komunikasi adalah area-area yang perlu meningkatkan kepatuhan. Sedangkan area yang menunjukkan tingkat kepatuhan yang lebih tinggi terhadap standar ISO 27001:2022 hanya pada satu area saja yaitu area Keamanan Fisik dan Lingkungan.

G. Rekomendasi dan Perbaikan

Berikut adalah beberapa rekomendasi dan perbaikan yang dapat dilakukan:

1) Manajemen Risiko:
   a. Meninjau ulang proses identifikasi risiko, penilaian risiko, dan pengelolaan risiko untuk memastikan kepatuhan dengan prinsip-prinsip ISO 27001:2022.
   b. Memastikan bahwa strategi mitigasi risiko yang tepat diimplementasikan dan diikuti oleh perguruan tinggi.
2) Kebijakan Keamanan Informasi:
   a. Meninjau dan memperbaharui kebijakan keamanan informasi untuk memastikan kesesuaian dengan standar ISO 27001:2022.
   b. Memastikan kebijakan mencakup semua persyaratan penting dalam pengelolaan keamanan informasi.
3) Aset Informasi:
   a. Mengidentifikasi dan mengklasifikasikan semua aset informasi yang dimiliki oleh perguruan tinggi.
   b. Memastikan adanya prosedur yang jelas untuk perlindungan, pemeliharaan, dan penghapusan aset informasi yang relevan.
4) Pengendalian Akses:
   a. Meninjau dan memperbaharui kebijakan dan prosedur pengendalian akses untuk memastikan kepatuhan dengan persyaratan ISO 27001:2022.
   b. Mengimplementasikan mekanisme pengendalian akses yang tepat, seperti autentikasi, manajemen hak akses, dan pemantauan aktivitas masing-masing pengguna.
5) Keamanan Jaringan dan Komunikasi:
   a. Meninjau kembali infrastruktur jaringan dan konfigurasi keamanan untuk memastikan kepatuhan dengan standar ISO 27001:2022.
   b. Menerapkan teknologi dan protokol keamanan yang tepat, seperti firewall, penerapan enkripsi, dan tindakan perlindungan lainnya untuk melindungi jaringan dan komunikasi.
6) Manajemen Insiden Keamanan:
   a. Menetapkan prosedur respons insiden yang jelas dan selalu terdokumentasi.
   b. Melatih tim respons insiden secara rutin dan memastikan koordinasi yang efektif dalam menangani insiden keamanan.

IV. SIMPULAN

Berdasarkan hasil evaluasi terhadap tingkat kepatuhan Salah satu perguruan tinggi yang ada di Kota Jambi terhadap standar ISO 27001:2022, berikut adalah kesimpulan terkait dengan pengembangan model penilaian kepatuhan organisasi tersebut: 1) Model penilaian kepatuhan yang dikembangkan telah memberikan gambaran mengenai tingkat kepatuhan Perguruan Tinggi tersebut terhadap standar ISO 27001:2022. Melalui penggunaan indikator yang telah ditentukan, evaluasi dapat dilakukan secara sistematis dan objektif. 2) Model penilaian ini memperlihatkan bahwa terdapat area-area di mana Perguruan Tinggi tersebut telah mencapai tingkat kepatuhan yang tinggi, seperti keamanan fisik dan lingkungan. Hal ini menunjukkan adanya upaya dan implementasi yang efektif dalam aspek tersebut. 3) Namun, ada juga area-area yang menunjukkan tingkat kepatuhan yang rendah atau sedang, seperti kebijakan keamanan informasi, manajemen risiko, aset informasi, pengendalian akses, keamanan jaringan dan komunikasi, serta manajemen insiden keamanan. Pada area-area ini, perlu dilakukan perbaikan dan peningkatan guna mencapai tingkat kepatuhan yang lebih baik. 4) Dalam pengembangan model penilaian, metode-metode pengumpulan data seperti wawancara, survei, observasi, dan analisis dokumen telah digunakan. Hal ini membantu dalam mendapatkan informasi yang dibutuhkan untuk evaluasi kepatuhan. 5) Berdasarkan hasil evaluasi, rekomendasi perbaikan dan peningkatan telah diberikan untuk masing-masing area yang memerlukan perhatian lebih. Implementasi dan evaluasi terhadap rekomendasi tersebut menjadi langkah penting dalam memperbaiki tingkat kepatuhan organisasi terhadap standar ISO 27001:2022.

UCAPAN TERIMA KASIH

Terima kasih kepada pihak-pihak yang telah mendukung terlaksananya kegiatan penelitian ini. Dukungan dari pihak perguruan tinggi tempat observasi atas kesediaannya dalam memberikan informasi saat wawancara serta antusias dalam

pengisian kuesioner yang diberikan. Terimakasih kepada seluruh tim redaksi Jurnal Teknik Informatika dan Sistem Informasi (JuTISI) yang telah membantu dan mengarahkan untuk terbitnya artikel ini.

DAFTAR PUSTAKA

[1] H. Wahyudi, A. Zulianto and A. Maulana, "Audit Keamanan Sistem Informasi Manajemen Akademik dan Kemahasiswaan Menggunakan SNI ISO/IEC 27001:2013," *Jurnal Computech & Bisnis*, vol. 14, no. 1, pp. 40-46, 2020.

[2] M. P. Mokodompit and N. Nurlaela, "Evaluasi Keamanan Sistem Informasi Akademik Menggunakan ISO 17799:2000 (Studi Kasus Pada Perguruan Tinggi X)," *Jurnal Sistem Informasi Bisnis*, vol. 6, no. 2, p. 97, 2017.

[3] F. A. Basyarahil and dkk, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO-IEC 27001-2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya," *Jurnal Teknik ITS*, vol. 6, no. 1, p. 122, 2017.

[4] R. R. Wijayanti, "Implementasi Octave-S Dan Standar Pengendalian ISO 27001:2013 Pada Manajemen Risiko Sistem Informasi Perguruan Tinggi," *Jurnal PETIR*, vol. 11, no. 2, p. 221, 2018.

[5] F. Pereira, P. Crocker and V. R. Leithardt, "PADRES: Tool for PrivAcy, Data REgulation and Security," *SoftwareX*, vol. 17, p. 1, 2022.

[6] G. Fox, T. Lynn and P. Rosati, "Enhancing consumer perceptions of privacy and trust: a GDPR label perspective," *Information Technology and People*, vol. 35, no. 8, pp. 181-204, 2022.

[7] Y. Kurii and I. Opirskyy, "ISO 27001: Analysis Of Changes And Compliance Features Of The New Version Of The Standard," *Cybersecurity: Education, Science, Technique*, vol. 3, no. 19, pp. 46-55, 2023.

[8] M. Bahrudin and Firmansyah, "Manajemen Keamanan Informasi di Perpustakaan Menggunakan Framework SNI ISOIEC-27001," *Perpustakaan Nasional*, vol. 25, no. 1, p. 46, 2018.

[9] M. Bakri and N. Iramayana, "Analisis Dan Penerapan Sistem Manajemen Keamanan Informasi Simhp Bpkp Menggunakan Standar ISO 27001," *Jurnal Tekno Kompak*, vol. 11, no. 2, p. 41, 2017.

[10] S. T. Yuwono, N. Pratama and V. Afifah, "Re-Assessment Konsistensi Dokumen Kontrol Sertifikasi ISO 27001:2013 (ISMS) di Bagian Komunikasi Satelit Monitoring PT. Bank BRI, TBK," *Jurnal IKRAITH-Informatika*, vol. 6, no. 2, p. 21, 2022.

[11] N. Hidaya and I. Jatnika, "Perancangan Sistem Manajemen Keamanan Informasi Data Center Standard SNI ISO IEC 27001 2013," *JUSIM (Jurnal Sistem Informasi Musirawas)*, vol. 7, no. 1, p. 24, 2022.

[12] H. Haikal, R. H. Ananza, I. Darmawan and R. Mulyana, "Perancangan Tata Kelola Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik (SPBE) Menggunakan Standar ISO 27001:2013 (Studi Kasus: Diskominfotik Kabupaten Bandung Barat) Design Of Information Security Governance For E-Government Using ISO 27001:20," in *e-Proceeding of Engineering*, Bandung, 2019.

[13] M. Budhiningtias Winanti and I. Dzulhan, "Audit Keamanan Sistem Informasi Akademik Dengan Kerangka Kerja ISO 27001 Di Program Studi Sistem Informasi Unikom," *UNIKOM*, vol. 16, no. 2, p. 122, 2020.

[14] M. Kartika, S. A1, Y. Saintika and W. A. Prabowo, "Penyusunan Manajemen Risiko Keamanan Informasi Dengan Standar ISO 27001 Studi Kasus Institut Teknologi Telkom Purwokerto," *JUSTIN (Jurnal Sistem dan Teknologi Informasi)*, vol. 10, no. 4, p. 423, 2022.

[15] W. C. Pamungkas and F. T. Saputra, "Evaluasi Keamanan Informasi Pada SMA N 1 Sentolo Berdasarkan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001:2013," *Jurnal Sistem Komputer dan Informatika (JSON)*, vol. 1, no. 2, pp. 101-106, 2020.

[16] D. Drljača and B. Latinović, "Frameworks for Audit of an Information System in Practice," *JITA - Journal of Information Technology and Applications (Banja Luka) - APEIRON*, vol. 6, no. 2, p. 78, 2017.

[17] P. R. I. 2.-D. P. R. R. I. d. P. R. INDONESIA, Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, Jakarta, 2022.