BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Sebelumnya

Kajian terhadap penelitian sebelumnya dilakukan untuk memberikan pemahaman yang lebih mendalam tentang strategi prioritas peningkatan tata kelola TI yang berlaku untuk mendukung penelitian ini. Penelitian-penelitian sebelumnya yang digunakan untuk menyusun penelitian ini adalah sebagai berikut:

1. **Analisis Tingkat Kematangan (Maturity Level) dan PDCA (Plan-Do-Check-Act) Dalam Penerapan Audit Sistem Manajemen Keamanan Informasi Pada PT Indonesia Game Menggunakan Metode ISO 27001:2013**[9]**.**

   PT Indonesia Game salah satu perusahaan yang berorientasi mengenai *game* dan menggunakan *cloud system* untuk bisnisnya. Merujuk pada penggunaan *cloud system* diperlukan keamanan informasi yang efektif agar proses bisnis pada PT Indonesia *Game* berjalan sesuai dengan tujuan perusahaan. PT Indonesia *Game* melakukan tindakan audit secara berkelanjutan baik dengan audit internal maupun eksternal. Permasalahan dalam penelitian ini adalah telah terdekteksi adanya ketidaksesuaian antara dokumen intruksi kerja yang berkaitan dengan *labelling* tidak ditemukan telah terdaftar pada dokumen utama.Penelitian ini berfokus untuk melakukan audit manajemen keamanan informasi pada PT Indonesia *Game* dengan standar ISO 27001:2013. Berdasarkan analisis yang telah dilakukan pihak audit PT Indonesia *Game* memiliki tingkatan paling rendah pada *Annex* 7 diantara *Annex* lainnya dikarenakan ditemukan ada beberapa dokumen utama yang tidak berlabel dan ada beberapa formulir yang tidak sesuai dengan prosedur yang tercantum pada judul sehingga tidak sinkron. Namun, secara totalitas ISO 2001:2013 yang telah ditetapkan

secara baik karena memiliki nilai *mean* 94,45% dengan level 5 *Optimised* [9].

2. **Hasil Penilaian Risiko Keamanan Informasi pada Laboratorium Klinik Berdasarkan Kriteria Kendali Dalam Penerapan ISO 27001** [10]**.**

   Laboratorium klinik sebagai institusi kesehatan diperlukan perlindungan data yang vital seperti adanya data aset informasi yang mencakup data pasien dan lain sebagainya. Sebagai pendorong dalam pengefisienkan proses bisnis dari laboratorium klinik dilakukan transformasi ke proses digitalisasi agar memaksimalkan transaksi dari luar laboratorium utamanya. Proses digitalisasi memiliki risiko yang tidak kalah besar dengan proses secara manual. Proses adminitrasi secara digital dirasa rawan akan tindakan peretasan ataupun kejahatan siber lainnya. Laboratorium klinik telah mengalami kejahatan siber berdasarkan wawancara dengan manajemenn yaitu telah terjadi peristiwa kebocoran data karyawan lalu dimanfaatkan oleh oknum tidak bertanggung jawab. Perhatian utama dalam penelitian ini yaitu menerapkan pengendalian teknis untuk mengamankan informasi pada laboratorium klinik. Metode pengumpulan data yang digunakan dalam penelitian ini yaitu metode kualitatif untuk pengumpulan data secara penyebaran survei menggunakan kuisioner serta wawancara untuk menggali informasi. Setelah itu dilakukan proses interpretasi untuk membuat kesimpulan. Lalu dilanjutkan dengan proses penilaian proses bisnis organisasi dengan menetapkan tabel risiko sebagai hasil penelitian. Berdasarkan penelitian disimpulkan bahwa klinik laboratorium telah teridentifikasi sebanyak 35 risiko pada departemen *business development & Information Technology* yang berkategori moderat dengan cakupan kebutuhan yang terkendali yang banyak berdasarkan ISO/IEC 27001:2013 [10].

3. **Analisis Penilaian Risiko Keamanan Informasi Berdasarkan Iso 27005 Untuk Persiapan Sertifikasi Iso 27001 pada Pemerintah Kota Madiun**[11]

   Dinas Komunikasi dan Informatika Kota Madium memili fungsi untuk proses pelayanan masyarakat di bidang teknologi informasi. Memiliki fokus utama untuk menjamin bahwa data masyarakat dan pemerintah aman, rahasia, utuh, dan selalu tersedia. Saat ini masih terdapat minimnya kewaspadaan signifikansinya dalam penjagaan keamanan informasi yang memiliki dampak buruk jika tidak diwaspadai secara dini dapat membuka peluang kejahatan dunia maya seperti data bocor, rusak, tidak akurat, atau hilangnya data yang penting. Berdasarkan itu dibutuhka adanya prosedur penanganan risiko sebagai langkah tindakan preventif untuk mengidentifikasi segala potensi dan peluang risiko yang mungkin terjadi. Penelitian ini menggunakan model ISO/IEC 27001:2013, ISO/IEC 27002:2013, dan ISO/IEC 2700:2013 yang mengutamakan pembuatan tata kelola risiko keamanan informasi. Berdasarkan pembahasan hasil disimpulkan bahwa Dinas Komunikasi dan Informatika Kota Madiun dikategorikan dalam beberapa level yaitu *very low, low,* dan *high.* Dengan masing masing risiko nilai RPN 16, 30 dan 56, dan 84 dan 96. Berdasarkan pemetaan ISO 27001:2013 dan ISO 27005:2013 disimpulkan SOP yang ada pada Dinar Komunikasi dan Informatika sudah baik sebesar 35 dan sejumlah 1 SOP diperlukan perbaikan pada bagian penilaian insiden yang harus terpenuhi pada ISO 27001:2013 dan ISO 27005:2013 yang berjumlah 22 [11].

4. **Penanganan Risiko Keamanan Informasi Aplikasi Webmarket Berdasarkan ISO 27001:2013 (Study Kasus pada PT Sanjaya Citra Anugrah)**[12]

   PT Sanjaya Citra Anugrah merupakan perusahaan yang bergerak pada persewaan alat berat. Perusahaan ini berkomintmen dalam menjaga kerahasiaan data pelanggan. Berdasarkan hal tersebut dibutuhkan penyusunan keamanan informasi yang memiliki fokus utama dalam

meminimalisir dan menurunkan risiko keamanan informasi yang akan datang. Dilakukan tindakan implementasi keamanan informasi menggunakan ISO 27001:2013 untuk melindungi keamanan informasi. Setelah wawancara ditemukan isu internal seperti adanya sistem pada dokumentasi operasional yang belum dilengkapi sesuai dengan persyaratan standar keamanan, minimnya pengendalian pada sistem informasi dan terdapat banyak fitur keamanan yang kurang memenuhi standar. PT SCA menyimpulkan risiko yang bernilai rendah dapat diterima. Namun untuk risiko yang bernilai sedang, tinggi, dan esktrim dilakukan tindak lanjut dengan persetujuan manajemen puncak PT SCA. Berdasarkan penelitian telah ditetapkan bahwa ditemukan 6 area dengan risiko 20 dan ditemukan beserta penyebab terjadi risiko dan dampak yang ditimbulkan pada faktor keamanan informasi. Tindakan preventif untuk menangani jika terjadi kejadian berulang perlu disusun rencana penanganan risiko dan diperoleh 14 rencana yang akan diterapkan perusahan berdasarkan ISO 27001:2013 yang diterapkan untuk mengurangu terjadinya risiko [12]

5. **Audit Keamanan Sistem Informasi Manajemen Akademik dan Kemahasiswaan Menggunakan SNI ISO/IEC 27001:2013**[13]

   Dunia pendidikan khususnya perguruan tinggi memiliki peranan signifikan dalam mengembangkan ilmu pengetahuan dan teknologi pada masyarakat sehingga diperlukan keterbaruan dan kemudahan dalam pencarian sumber informasi yang terbaru di masa kini. Masalah pada penelitian ini yaitu masih terdapat masalah seperti tidak dapat diakses dari luar oleh mahasiswa, dosen, maupun karyawan pada sistem pengoperasiannya, tidak tersinkronisasi dengan *website* ppdikti riset, pada penginputan nilai oleh dosen tidak adanya batasan waktu, adanya pelanggaran keamanan data yang menyebabkan data disebarkan oleh oknum tidak bertanggung jawab yang menyebabkan kerugian yang besar bagi perguruan tinggi. Berdasarkan hal tersebut diperlukan sebuah sistem untuk melakukan proses administrasi yang dapat menjaga keamanan informasi untuk mencegah adanya kejahatan siber yang mungkin terjadi dan memberikan

tempat dalam proses pendokumentasian data untuk pengoptimalan sistem pengarsipan pada perguruan tinggi. Penelitian ini menggunakan metode kualitatif dengan pendekatan studi kasus. Hasil dari penelitian ini telah diidentifikasikan mengenai klausul yang diterapkan yaitu *annex 5:* kebijakan keamanan, *annex 7* : manajemen asset, *annex 9* : kontrol akses, dan *annex 15* : kepatuhan. Berdasarkan hasil yang telah diteliti pada *annex* 5 mengenai kebijakan keamanan pada STMIK Mardira Indonesia masih adanya kesesuaian yang belum tercapai. Berdasarkan *annex 7* : manajemen asset pada STMIK Mardira Indonesia ditemukan ketidaksesuaian surat mengenai kebijakan pengelolaan aset yang digunakan dalam pencapaian dan pemeliharaan perlindungan yang sesuai pada asset organisasi. Pada *annex* 11 diperlukan pembentukan kebijakan yang jelas dan mencegah penyalahgunaan hak akses, dengan menerapkan prosedur pengendalian hak akses untuk menghindari akses yang tidak sah terhadap informasi dan fasilitas sistem informasi. Lalu penelitian ini juga menyimpulkan pada *annex* 15 mengenai kepatuhan Aktivitas yang dijalankan dalam sistem informasi akademik masih belum diadaptasi dengan baik pada aturan akademik yang telah ditetapkan dan kalender pendidikan yang telah diatur sebelumnya tidak sesuai dengan waktu yang telah dijadwalkan[13].

6. **Re-Assessment Konsistensi Dokumen Kontrol Sertifikasi ISO 27001:2013 (ISMS) di Bagian Komunikasi Satelit Monitoring PT. Bank BRI, TBK**[14]

   Penelitian ini dilaksanakan pada PT Bank BRI TBK yang berfokus pada divisi IT *Infrastructure & Operatins division* khususnya *Satellite Service Operations Department* sebagai organisasi yang telah menerapkan standar ISO 27001:2013 dalam kebijakannya, tentu memiliki tanggung jawab untuk memastikan bahwa seluruh *stakeholder* dan anggota tim, termasuk karyawan dan manajemen, memiliki pemahaman, penerapan, ketaatan, dan pelaksanaan terus-menerus terhadap prosedur manajemen keamanan informasi tersebut. Ini termasuk anggota tim pengganti, seperti karyawan yang baru bergabung. Sewaktu 2019 sempat terjadi *Covid-19*

yang mengakibatkan seluruh kegiatan dirumahkan oleh atas perintah para pemangku kepentingan. Hal ini menyebabkan diperlukannya tindakan pencegahan pada keamanan sistem informasi agar kegiatan bekerja dari rumah tersebut tidak mengalami kendala. Dalam konteks ini, salah satu solusi yang harus ditekankan adalah meningkatkan pendidikan dan kesadaran staff terkait dengan isu keamanan siber serta tindakan mitigasinya. Temuan penelitian ini meliputi penilaian kelayakan penerapan klausul dan dokumen pengendalian Sistem Manajemen Keamanan Informasi (SMKI), mengacu pada ISO/IEC 27001:2013, pada bagian pemantauan komunikasi satelit. Evaluasi terhadap parameter "Dilaksanakan" menunjukkan bahwa aspek tersebut telah diatur dalam prosedur dan kebijakan organisasi. Namun, penerapannya yang konsisten mungkin dipengaruhi oleh hubungannya dengan otoritas eksternal, bagian, atau fungsi di luar pengendalian internal. Sebaliknya pada parameter "*Frequenly*" menunjukkan bahwa penerapan internal pada Bagian Monitoring Satelit Komunikasi secara umum dilakukan, namun tidak terstandarisasi karena adanya praktik wajib dan terstandar dari seluruh perusahaan. Terhadap parameter "Selalu" dalam operasional, penilaian menunjukkan bahwa hal ini merupakan aspek yang sangat penting dalam pengelolaan data, informasi, dokumen, dan prosedur, yang secara konsisten ditekankan, diterapkan, dan dimanfaatkan sebagai pedoman dalam operasional. Saat menilai konsistensi penerapan klausul dan dokumen pengendalian ISO/IEC 27001:2013, diperoleh skor 81% untuk pengendalian risiko Tim atau Karyawan Baru, dan 90% untuk pengendalian risiko Pihak Ketiga. Berdasarkan data evaluasi yang dikumpulkan, dapat disimpulkan bahwa implementasi klausul, dokumen pengendalian ISO 27001:2013 (ISMS), dan kebijakan di Bagian Pemantauan Komunikasi Satelit (Manajer, Insinyur, Operator) menunjukkan tingkat konsistensi yang tinggi. Seluruh anggota tim memahami hak dan tanggung jawabnya, menjalankan tugasnya secara konsisten, dan memikul tanggung jawab untuk menjaga keamanan

informasi sejalan dengan prinsip Sistem Manajemen Keamanan Informasi (SMKI) [14].

7. **Evaluasi Keamanan Informasi Data Center Berdasarkan Standar ISO 27001:2013 (Studi Kasus PT. Pupuk Kalimantan Timur)**[15]

   PT. Pupuk Kalimantan Timur (PKT) adalah salah satu entitas bisnis yang berasal dari PT. Pupuk Indonesia, didirikan untuk memenuhi permintaan pupuk baik di dalam maupun di luar negeri. PKT juga dilengkapi dengan pusat data yang berfungsi sebagai penyimpan informasi penting yang perlu dijaga kerahasiaannya. Masalah yang ada pada penelitian ini yaitu telah terjadinya penyerangan pada data *center* yang yang menyebabkan dampak buruk yaitu proses pemasaran terganggu. Berdasarkan hasil penelitian ini diperoleh hasil bahwa kelengkapan dan kematangan keamanan informasi pada perusahaan ini telah berada pada tingkat empat *(define process).* Lalu penilaian risiko pada perusahaan ini menggunakan metode FMEA. Didapatkan 14 risiko yang berada pada tingkat *very low*, 2 risiko berada pada tingkatan *low,* dan 2 risiko berada pada tingkatan *high.* Berdasarkan hasil analisis direkomendasikan bahwa perusahaan perlu menerapkan beberapa kebijakan antara lain dilakukukan evaluasi terkait keamanan informasi, melakukan pembaharuan kebijakan yang lebih sesuai, melakukan pengelolaan inventaris, dan menetapkan kebijakan yang baru dalam penggunaan aset yang memperhitungkan para staff dan pihak ketiga [15].

8. **Designing a model to protect documented information according to the integration of some international standards (ISO 27001: 2013) (ISO 10013: 2021): A case study**[16]

   Irak memiliki komoditas unggulan yaitu sektor minyak dan gas yang menjadi sumber perekonomian negara Irak. Hal tersebut dibutuhkan perhatian mengenai informasi minyak yang terdokumentasi. Penelitian ini mengulas integrasi antara persyaratan beberapa ketentuan dari dua standar internasional, yaitu ISO 27001:2013 dan ISO 10013:2021. Tujuan penelitian ini adalah untuk menilai sejauh mana penerapan persyaratan dan

pedoman dari kedua standar tersebut, serta mempertimbangkan kemungkinan adopsi dan kepatuhannya di perusahaan eksplorasi minyak. Penelitian ini terbagi menjadi tiga bagian. Bagian awal membahas perlindungan informasi terdokumentasi, sementara bagian kedua mengeksplorasi dua standar internasional, yaitu ISO 10013:2021 dan ISO 27001:2013. Bagian ketiga menitikberatkan pada aspek praktis dari informasi terdokumentasi. Masalah dalam penelitian ini yaitu lemahnya perlindungan terhadap informasi terdokumentasi pada perusahaan minyak di Irak. Berdasarkan penelitian ini didapatkan beberapa rekomendasi untuk menggunakan perangkat pendokumentasian secara elektronik agar proses pendokumentasian selalu *up to date,* perusahaan mulai menerapkan standar keamanan informasi agar mencapai batas pantas mendapatkan sertifikasi keamanan informasi dan mulai melakukan klasifikasi dokumen secara elektronik agar mengurangi risiko yang mungkin terjadi [16].

9. ***Integration of ITIL V3, ISO 20000 & ISO 27001:2013forIT Services and Security Management System***[17]**.**

   Organisasi TI bertanggung jawab atas penyediaan layanan TI yang berkualitas dan menjaga keamanan TI guna meningkatkan daya saing mereka. Keamanan dan layanan TI keduanya memiliki standar dan kerangka kerja internasional yang masing-masing. Implementasi sistem manajemen layanan TI (SMS) dan sistem manajemen keamanan informasi (SMKI) secara terpisah dapat mengakibatkan penggunaan sumber daya yang tinggi dan biaya yang signifikan. Oleh karena itu, para pemimpin perlu menjalankan dan menyelaraskan sistem tersebut. Dalam konteks ini, makalah ini akan difokuskan pada integrasi ISO 20001 sebagai standar SMS, ITIL v3 sebagai kerangka kerja, dan ISO 2700s1 sebagai standar ISMS. Akan dijelaskan bagaimana ITIL V3 dapat digabungkan dengan ISO 20001 dan ISO 27001 dengan memetakan kesamaan proses, prosedur, dan sumber daya secara ilmiah. Makalah ini memberikan panduan bagi organisasi TI yang berencana menerapkan standar dan kerangka kerja SMS dan SMKI. Lampiran bagian 4 menyajikan tabel persamaan proses,

prosedur, dan sumber daya, sehingga organisasi dapat menggunakan proses gabungan untuk mengurangi biaya penerapan standar tersebut. Penelitian ini mencari hubungan dengan ISO/IEC 2000 dan ISO/IEC 27001:2013 dan checklist 2000 dengan standar ISO/IEC 27001:2013 yang digunakan sebagai analisis dasar. Metode yang digunakan dalam penelitian ini yaitu mencari keterkaitan antar ISO dengan penilaian deskriptif caranya melakukan pengumpulan data dengan melihat dokumen yang ada dan observasi lapangan. Berdasarkan analisa peneliti bahwa implementasi sistem manajemen berdasarkan standar ISO, khususnya ISO 20000 dan ISO 27001, memerlukan komitmen dari dewan organisasi. Manajemen senior bertanggung jawab atas proses implementasinya, dan sebuah tim implementasi akan merancang rencana yang mencakup metodologi risiko, daftar risiko, dan mitigasi risiko. Kesadaran seluruh peserta yang terlibat dalam implementasi standar ISO juga penting, dengan pendidikan yang baik dalam keamanan informasi dan manajemen layanan. Pengendalian dokumen dan catatan, SOP, serta pedoman akan ditetapkan, memungkinkan metrik manajemen untuk mengukur efektivitas kontrol keamanan dan proses. Proses audit internal akan mendeteksi ketidaksesuaian dan tingkat implementasinya, sehingga dapat ditinjau oleh manajemen puncak. Terakhir, tindakan perbaikan dan pencegahan diperlukan untuk perbaikan berkelanjutan dalam sistem manajemen terpadu[17].

10. **Maturity Framework Analysis ISO 27001: 2013 on Indonesian Higher Education** [18]**.**

    Strategi yang efektif penerapan langkah yang dirancang mengatasi masalah keamanan dengan menekankan pada pengendalian internal, yang menyoroti hubungan antara prosedur organisasi dan langkah-langkah keamanan. Masalah pada penelitian ini yaitu terdapat celah pada keamanan sistem informasi yang dapat menyebabkan kerugian banyak pihak. Minimnya kesadaran akan penggunaan teknologi informasi serta cara pegawai dalam penanganan masalah yang dirasa kurang tepat. Berdasarkan

hal tersebut penelitian ini bertujuan untuk mengetahui kemampuan dan kesenjangan terhadap standar tata kelola yang ditetapkan secara internasional. Penelitian ini disimpulkan bahwa tingkat kematangan praktik keamanan informasi pada sistem informasi akademik perguruan tinggi di Indonesia berada pada level 2 *Managed Process* dan level 3 *Founded Process,* dengan komposisi 40% pada level 3 dan 60% pada level 2. Dapat disimpulkan bahwa sebagian besar perguruan tinggi di Indonesia belum sepenuhnya mampu menerapkan praktik keamanan informasi sesuai standar internasional. Jika dilihat dari masing-masing klausa atau domain, nilai gap antara nilai tingkat kematangan saat ini dengan nilai tingkat kematangan yang diharapkan berbeda-beda untuk setiap klausa (domain). Kesenjangan terkecil (1 level) terdapat pada klausul A5: Kebijakan Keamanan Informasi, klausul A9: Kontrol Akses, dan klausul A11: Keamanan fisik dan lingkungan. Kesenjangan terbesar (4 level) terdapat pada klausul A14: Akuisisi, pengembangan, dan pemeliharaan sistem dan klausul A18: kepatuhan. Untuk pengembangan penelitian SMKI, penilaian dapat dilakukan terhadap lebih dari 35 perguruan tinggi atau survei sebanyak yang diinginkan terhadap perguruan tinggi di Indonesia baik berdasarkan wilayah atau provinsi atau berdasarkan derajat akreditasi A atau B, dapat juga berdasarkan kategori universitas tersebut. seperti tingkat Universitas dan Institut dan bahkan tingkat departemen.

Berikut ini merupakan tabel hasil penelitian sebelumnya dengan metode ISO 27001.

Tabel 2. 1 Tinjauan Pustaka

No	Judul	Comparing	Contrasting	Criticize	Synthesize	Summarize
1.	Analisis Tingkat Kematangan (Maturity Level) dan PDCA (Plan-Do-Check-Act) Dalam Penerapan Audit Sistem Manajemen Keamanan Informasi Pada PT Indonesia Game Menggunakan Metode ISO 27001:2013[9].	Melakukan audit internal dengan menggunakan ISO 27001:2013.	Menggunakan analisis dengan Maturity Level dan PDCA (Plan-Do-Check-Act).	Dokumen terkait intruksi kerja labelling yang tidak terdaftar dalam dokumen utama tidak memiliki kesusuaian.	Menganalisis kesenjangan kinerja dengan berdasarkan standar yang berlaku.	Dengan adanya penilaian tingkat kematangan dapat meningkatkan kinerja bidang kearsipan dan membantu auditor serta dapat berjalan dengan sesuai kegiatan berdasarkan standar ISO 27001:2013.
2.	Hasil Penilaian Risiko Keamanan Informasi	Melakukan pendekatan menggunakan	Penilain risiko keamanan pelayanan digital	Diperlukan tindak lanjut mengenai ketetapan dari	Penilaian risiko harus dilakukan secara periodik.	Risiko keamanan informasi yang telah dinilai mempermudah

No	Judul	Comparing	Contrasting	Criticize	Synthesize	Summarize
	pada Laboratorium Klinik Berdasarkan Kriteria Kendali Dalam Penerapan ISO 27001[10]	ISO 27001 untuk menilai risiko.	pada laboratorium klinik	faktor kendali tambahan yang tepat.		dalam memahami proses perilaku secara menyeluruh
3.	Analisis Penilaian Risiko Keamanan Informasi Berdasarkan Iso 27005 Untuk Persiapan Sertifikasi Iso 27001 pada Pemerintah Kota Madiun[11]	Mengidentifikasi dan memberikan informasi terkait dengan kerentanan risiko, ancaman sistem, serta rekomentasi mitigasi	Membahas mengenai sistem E-Kinerja untuk mengukur dan menilai kinerja Apartur Sipil Negara (ASN).	Keterbatasan ruang lingkup dan informasi	Penilaian risiko yang dilakukan untuk membantu persiapan sertifikasi.	Rekomenda si SOP harus disusun sebagai upaya mitigasi risiko berdasarkan ISO 27001:2013.
4.	Penanganan Risiko Keamanan Informasi Aplikasi Webmarket Berdasarkan ISO	mengimplementasikan keamanan informasi berdasarkan ISO	Pengimplementasian ISO 27001:2013 untuk keamanan	Penyusunan rencana risiko kurang maksimal.	Penanganan risiko dibuat dengan menyusun rencana	Penyusunan rencana penanganan risiko menggunakan ISO 27001 :2013 sehingga

No	Judul	Comparing	Contrasting	Criticize	Synthesize	Summarize
	27001:2013 (Study Kasus pada PT Sanjaya Citra Anugrah)[12]	27001:2013 dalam mengidenntifikasikan risiko yang akan terjadi.	informasi pada PT Sanjaya Citra Anugrah		sesuai dengan ISO 27001:2013	keamanan informasi dapat terjaga dan pada akhirnya meningkatkan tingkat kepercayaan dari stakeholder.
5.	Audit Keamanan Sistem Informasi Manajemen Akademik dan Kemahasiswaan Menggunakan SNI ISO/IEC 27001:2013[13]	Mengaudit SIMAK agar terdokumentasi dan memperoleh bukti audit serta mengevaluasi secara objektif dengan menggunakan standar SNI ISO/IEC 27001:2013	Penulis menggunakan klausul 5 (security policy), klausul 7 (asset management), klausul 9 (access control) dan klausul 15 (compliance).	Penelitian hanya pada bagian audit keamanan sistem informasi.	Melakukan audit untuk mendapatkan bukti audit serta dilakukan evaluasi secara objektif.	Perkembangan teknologi secara cepat menghasilkan perubahan yang signifikan dalam kehidupan.

No	Judul	Comparing	Contrasting	Criticize	Synthesize	Summarize
6.	Re-Assessment Konsistensi Dokumen Kontrol Sertifikasi ISO 27001:2013 (ISMS) di Bagian Komunikasi Satelit Monitoring PT. Bank BRI, TBK[14]	Perlu dilakukannya perlindungan data informasi dari ancaman dan menjaga kerahasiaan data.	Pelaksanaan re-assessment yang dilakukan sesuai dengan kebijakan yang telah ditetapkan.	Tidak adanya konsistensi dan prosedur ada yang telah dijalankan ada yang belum dijalankan.	Kebijakan untuk pengelolaan data sensitif dilakukan secara sistematis.	Pemahaman mengenai hak dan kewajiban harus dilakukan secara bertanggungjawab serta konsisten agar keamanan informasi terjaga sesuai dengan kerangka sistem manajemen keamanan informasi
7.	Evaluasi Keamanan Informasi Data Center Berdasarkan Standar ISO 27001:2013 (Studi Kasus PT. Pupuk Kalimantan Timur)[15]	Mengevaluasi keamanan informasi dengan melihat hasil kematangan keamanan informasi	Penggunaan failure Mode and Effect Analysis (FMEA) untuk penilaian risiko.	Perlu dilakukan peningkatan dan evaluasi pada bidang keamanan informasi data center.	Menganalisis kesenjangan dengan sistem manajeman keamanan sistem.	Dalam peningkatan keamanan informasi untuk lebih optimal dilakukan Tindakan seperti peninjauan kebijakan keamanan informasi, inventatis

No	Judul	Comparing	Contrasting	Criticize	Synthesize	Summarize
						asset, control asset, keamanan fisik, dan keamanan operasi.
8.	*Designing a model to protect documented information according to the integration of some international standards (ISO 27001: 2013) (ISO 10013: 2021): A case study*[16]	Penelitian ini mengulas integrasi antara persyaratan beberapa ketentuan dari dua standar internasional, yaitu ISO 27001:2013 dan ISO 10013:2021.	Menerapkan model untuk mendiagnosis kesenjangan antara realitas aktual pekerjaan.	Tidak adanya pengklasifikasian dokumen.	Penanganan risiko dengan menggunakan ISO 27001:2013 dinilai efektif.	Sistem elektronik yang terpadu penting dilakukan sebagai upaya membangun sistem elektronik dengan alur kerja otomatis.
9.	*Integration of ITIL V3, ISO 20000 & ISO 27001:2013forIT Services and Security*	Menggunakan standar ISO 27001:2013 sebagai standar	Peneliti membahas mengenai ITIL V3 dan ISO 20000	Peneliti tidak menggunakan analisis integrasi yang diharapkan	Merancang dan mengembangkan formulir serta	Seluruh tim bertanggung jawab memiliki kesadaran dalam standar ISO.

No	Judul	Comparing	Contrasting	Criticize	Synthesize	Summarize
	Management System[19].	sistem manajemen keamanan informasi.	pada sistem manajemen layanan dan keamanan.	dapat menghemat sumber daya perusahaan.	mengenalisis korelasinya.	Proses audit internal memiliki peranan penting untuk mendeteksi ketidaksesuaian
10	*Maturity Framework Analysis ISO 27001: 2013 on Indonesian Higher Education* [18].	Pengendalian yang berfokus dalam keamanan informasi dengan menggunakan ISO 27001:2013.	Menghitung tingkat kematangan menggunakan SSE-CMM.	Masih terdapat kesenjangan antara praktik dengan kondisi yang diharapkan.	Penguran tingkat kematangan dilakukan sesuai prosedur.	Kontrol terhadap keamanan informasi diperlukan untuk memantau dan meningkatkan keamanan informasi organisasi.

Berdasarkan perbandingan Tabel 2.1 didapatkan proses pengukuran pada keamanan manajemen sistem informasi pada beberapa penelitian sebelumnya di lingkup perusahaan, perguruan tinggi, departemen, dan pemerintahan ataupun instansi lainnya pada penelitian itu diperoleh bahwa organisasi tersebut kurang maksimal dalam proses menjaga keamanan manajemen sistem informasi. Penelitian yang akan dilakukan oleh penulis berfokus untuk meningkatkan standarisasi keamanan sistem manajemen informasi organisasi. Penelitian ini dilakukan menggunakan ISO 27001:2013 untuk mengevaluasi mengenai keamanan sistem informasi pada PERUMDA Tirta Satria Kabupaten Banyumas untuk memaksimalkan keamanan sistem informasi. Pemilihan ISO 27001:2013 ini sebagai standar dalam melaksanakan evaluasi penelitian ini dikarenakan ISO sendiri merupakan standar internasional dalam penyelesaian masalah yang terjadi di PERUMDA Tirta Satria Banyumas, fleksibilitas dalam mengembangkan standar ini sangat dipengaruhi oleh persyaratan, tujuan, dan kriteria keamanan organisasi yang berbeda, serta kepatuhan terhadap standar nasional dan internasional SNI ISO 27001. Proses yang disederhanakan ini memfasilitasi pembuatan dan pengakuan Sistem Manajemen Keamanan Informasi (SMKI) baik di tingkat nasional maupun global.

2.2 Dasar Teori

Penelitian ini harus didasarkan pada landasan teori dari sumber yang tepat. Berikut beberapa dasar teori yang relevan menjadi penelitian ini antara lain yaitu:

2.2.1 Keamanan

Secara etimologis bahwa kata "keamanan" berasal dari bahasa Latin, yaitu *"securus*" (*se+cura*), yang artinya terbebas dari bahaya dan ketakutan. Kata ini juga dapat diartikan sebagai gabungan dari "se" yang berarti tanpa atau tanpa adanya, dan "*curus*" yang berarti kegelisahan. Berdasarkan penjelasan tersebut maka "keamanan" dapat diartikan sebagai pembebasan dari kegelisahan, atau situasi yang tenang tanpa risiko atau ancaman. Keamanan adalah kondisi bebas dari ancaman dan bahaya. Kondisi aman ini tidak hanya diinginkan oleh negara, tetapi juga oleh individu dan kelompok [20]. Setiap entitas, baik itu pemerintahan, organisasi, perusahaan, maupun masyarakat umum, berupaya untuk menciptakan lingkungan yang aman demi menjaga stabilitas, kenyamanan, dan kesejahteraan.

2.2.2 Sistem

Sistem merupakan suatu unsur-unsur yang saling berinteraksi secara terkait untuk mencapai suatu tujuan atau fungsi khusus. Unsur-unsur ini dapat mencakup komponen, proses, individu, data, energi, atau unsur lain yang bekerja sama untuk mencapai hasil yang diinginkan. Pada konteks yang lebih spesifik, sistem dapat merujuk pada serangkaian prosedur atau aturan yang terorganisir yang dirancang untuk mencapai tujuan atau mengatasi masalah. Sistem hadir di berbagai bidang, seperti ilmu komputer, manajemen, sains, teknologi, dan berbagai disiplin ilmu lainnya [21]. Misalnya, dalam ilmu komputer, sistem operasi mengelola perangkat keras dan perangkat lunak komputer untuk menyediakan layanan bagi program komputer.

2.2.3 Informasi

Informasi yaitu suatu data yang telah diolah atau diorganisir sehingga memiliki makna atau nilai yang berguna untuk proses pengambilan keputusan. Informasi berguna dalam pemanfaan pemecahan masalah, pengumpulan data, dan analisis kinerja. Informasi dapat didefinisikan sebagai suatu kelompok yang telah mengalami proses pengolahan sehingga memperoleh arti dan manfaat yang lebih luas. Merujuk pada pandangan para ahli tersebut, dapat disimpulkan bahwa informasi merupakan sekelompok data yang berasal dari sekumpulan fakta lalu setelah diolah dengan cara tertentu, dapat memiliki daya guna bagi pihak yang mengaplisikannya. Melalui sintesis pandangan para pakar tersebut, peneliti menyimpulkan bahwa informasi merupakan data yang telah melalui proses pengolahan sehingga membentuk suatu bentuk yang memiliki makna bagi pengguna dan memiliki nilai kebermanfaatan untuk proses pengambilan keputusan, baik saat ini maupun di masa mendatang [22]. Maka dari itu, informasi tidak hanya sekadar data yang terkumpul, tetapi telah diorganisir dan diinterpretasikan sehingga dapat digunakan untuk memahami situasi, mengidentifikasi pola atau tren, serta mendukung pengambilan keputusan yang lebih baik dan efektif.

2.2.4 Keamanan Informasi

Keamanan informasi merupakan suatu teknologi yang berguna dalam proses perlindungan data informasi terkait pengaksesan, penggunaan, perubahan, dan penyebaran [23]. Keamanan informasi ini dilakukan sebagai upaya pencegahaan pada suatu perusahaan dari ancaman luar seperti sabotase data dan lain-lain.

Fungsi keamanan informasi meliputi penilaian kesanggupan proses tata kelola keamanan informasi, serta peran, tugas, dan tanggung jawab manajer keamanan informasi di dalam instansi, perusahaan, atau fungsi. Demikian pula dengan manajemen risiko keamanan informasi

yang berfungsi untuk mengkaji kesanggupan proses implementasi manajemen risiko sebagai pedoman pengimplementasian dalam strategi keamanan informasi[4]. Pendekatan ini mencakup langkah-langkah seperti penerapan kontrol keamanan yang sesuai, pemantauan terus-menerus terhadap ancaman baru, serta respons cepat terhadap insiden keamanan jika terjadi.

2.2.5 ISO 27001:2013

ISO/IEC 27001:2013 merupakan standarisasi keamanan yang diakui secara global dan disajikan dengan metode yang berbeda. Pembangunan sistem manajemen keamanan informasi harus dilakukan dengan menerapkan standar keamanan yang terkontrol dan selaras dengan ISO/IEC 27001:2013. Pada proses mempertahankan rahasia, ketersediaan, dan integritas informasi mengimplementasikan prosedur manajemen risiko adalah fungsi utama dari Sistem Manajemen Keamanan Informasi (SMKI). Ini memastikan bahwa risiko-risiko tersebut dikelola dengan efisien dan diminimalkan oleh pihak yang memiliki kewenangan [4]. Adapun Klausa dalam ISO/IEC 27001: 2013 terdiri dari 10 yaitu[14]:

1. Klausa 1 – Ruang Lingkup Standar

Standar Internasional ini menetapkan ketentuan yang harus dilakukan sebagai proses pengendalian, pemeliharaan, pengimplementasian dan terus dilakukan sebagai upaya peningkatan sistem manajemen keamanan informasi dalam konteks organisasi. Standar Internasional ini termasuk dalam ketentuan sebagai salah satu aspek evaluasi dan tindakan risiko keamanan informasi yang disamakan dengan kebutuhan organisasi. Ketentuan yang terdapat dalam Standar Internasional ini memiliki sifat *general* dan diperuntukan berlaku pada segala jenis, ukuran, atau sifat organisasi tanpa terkecuali.

2. Klausa 2 – Referensi Normatif

Referensi normatif yaitu seperangkat norma atau peraturan yang merujuk perusahaan dalam beroperasi sesuai dengan pedoman hukum yang berlaku.

3. Klausa 3 – Ketentuan dan Definisi

Ketentuan dan definisi yang dimaksud yaitu pemahaman mendalam mengenai proses dan kriteria untuk menentukan keamanan informasi perusahaan. Perusahaan mengetahui mengenai kebijakan keamanan informasi dengan mengidentifikasikan kriteria organisasi dalam upaya menentukan ketetapan dan definisi spesifik yang berlaku.

4. Klausa 4 – Konteks Organisasi

Klausa 4 ini terbagi menjadi beberapa *sub* bab antara lain :

a. Memahami organisasi dan konteksnya

Berisi mengenai penentuan isu-isu organisasi baik eksternal maupun intenal yang sesuai dengan tujuan dan kemampuan organisasi dalam proses pencapaian tujuan.

b. Memahami kebutuhan dan harapan dari beberapa pihak yang memiliki kepentingan

Pemahaman permintaan kedepannya oleh para pihak-pihak yang berkepentingan dan penentuan ruang lingkup sistem menajemen keamanan informasi juga dibahas pada konteks organisasi.

c. Menentukan ruang lingkup sistem manajeman keamanan informasi

Organisasi mampu menentukan batasan mengenai ruang lingkup untuk penerapan sistem manajemen keamanan informasi.

d. Kemanan Manajemen Sistem Informasi

Organisasi perlu memaksimalkan sistem manajemen keamanan sistem informasi dengan cara melakukan penerapan, pemeliharan sesuai dengan syarat ISO 27001:2013.

5. Klausa 5 – Kepemimpinan

Klausa 5 ini terbagi menjadi beberapa *sub* bab antara lain :

a. Kepeminpinan dan komitmen

Kepemimpinan dan komitmen harus ditunjukan sejalan dengan sistem manajeman keamanan informasi dengan penetapan kebijakan keamanan informasi yang sesuai dengan tujuan organisasi dan melindungi keamanan informasi. Perusahaan harus memiliki jajaran manajemen puncak organisasi yang memiliki peranan serta tanggung jawab dan kewenangan yang sesuai dengan keamanan informasi.

b. Kebijakan

Para pihak menajemen organisasi mampu menerapkan kebijakan keamanan informasi sejalan dengan tujuan organisasi perusahaan dengan melibatkan tujuan keamanan informasi dan menyediakan kerangka kerja bagi keberlangsungan tujuan keamanan informasi.

c. Peranan, tanggungjawab dan kewenangan organisasi

Pimpinan perusahaan perlu memverifikasi penugasan dan komunikasi tanggung jawab dan wewenang terkait keamanan informasi. Hal ini dilakukan untuk menjamin kepatuhan sistem manajemen keamanan informasi dengan persyaratan standar internasional. Selain itu, mereka diharapkan memberikan laporan tentang kinerja sistem manajemen keamanan informasi kepada pimpinan perusahaan.

6. Klausa 6 – Perencanaan

a. Tindakan mengatasi resiko dan peluang

Perencanaan dibutuhkan sebagai tindakan mengatasi risiko dan peluang. Organisasi juga perlu menetapkan informasi perencanaan untuk mencapai tujuan keamanan informasi.

i. Umum

Saat merancang sistem manajemen keamanan informasi, organisasi perlu memperhitungkan kekhawatiran dan prasyarat,

menilai risiko dan peluang, dan mengidentifikasi langkah-langkah yang dibutuhkan dalam memverifikasi bahwa sistem dapat mewujudkan hasil yang diinginkan. Hal ini melibatkan pencegahan atau mitigasi konsekuensi yang tidak diinginkan dan upaya untuk perbaikan berkelanjutan.

ii. Penilaian risiko keamanan informasi

Organisasi harus menetapkan dan menerapkan prosedur untuk mengevaluasi risiko yang berkaitan dengan keamanan informasi. Prosedur ini perlu menguraikan, memetakan dan merawat standar risiko keamanan informasi, melibatkan kriteria penerimaan risiko dan petunjuk pelaksanaan evaluasi risiko keamanan informasi.

iii. Perlakukan risiko keamanan informasi

Organisasi perlu menerapkan prosedur untuk mengatasi risiko keamanan informasi. Hal ini memerlukan pemilihan opsi yang tepat untuk mengatasi risiko-risiko ini, dengan mempertimbangkan hasil penilaian risiko. Prosesnya mencakup mengidentifikasi semua pengendalian yang diperlukan untuk menerapkan perlakuan risiko, menilai pengendalian tersebut, membuat pernyataan implementasi yang menjelaskan pengendalian yang diperlukan, merumuskan rencana perlakuan risiko keamanan informasi, mendapatkan perizinan dari pemilik risiko untuk rencana tersebut, dan mengidentifikasi keamanan informasi yang tersisa.

b. Pencapaian dan perencanaan tujuan keamanan informasi

Organisasi perlu menerapkan tujuan keamanan informasi pada fungsi dan tingkat yang relevan. Tujuan-tujuan ini mampu selaras dengan kebijakan keamanan informasi, harus mempertimbangkan persyaratan keamanan informasi yang relevan, dan ditentukan melalui penilaian risiko.

7. Klausa 7 – Pendukung

   Pendukung suatu organisasi seperti dukungan sumber daya, dukungan kompetensi, kesadaran, komunikasi, informasi yang terdokumentasi perlu dilakukan untuk pembentukan, penerapan, pemeliharaan, dan peningkatan keberlanjutan dalam keamanan sistem manajemen keamanan informasi.

8. Klausa 8 – Operasi

   a. perencanaan operasi dan control

      Organisasi perlu merencanakan dan pengendalian operasi untuk menerapkan tindakan yang akan dilakukan. Organisasi harus melakukan pengendalian perubahan agar tidak memperbesar dampak buruk jika diperlukan.

   b. Penilaian risiko keamanan informasi

      Organisasi diharuskan untuk melakukan penilaian risiko keamanan informasi secara berkala atau jika terjadi perubahan besar yang diusulkan atau terjadi, dengan mempertimbangkan kriteria yang telah ditentukan.

   c. Perlakuan risiko keamanan informasi

      Organisasi mampu mengimplementasikan perencanaan untuk melindungi dan mencegah dari hal hal yang mengancam keamanan informasi.

9. Klausa 9 – Evaluasi Kinerja

   a. Pemantauan, pengukuran, analisis dan evaluasi

      Organisasi mampu melakukan harus memantau, mengukur, serta mengevaluasi kinerja yang ada di suatu organisasi

   b. Audit internal

      Organisasi harus mengevaluasi kinerja keamanan sistem dan keefektifitasannya dengan melakukan audit internal dan melakukan tinjauan manajemen untuk memverifikasi kesesuain serta kecukupan, akan keberlanjutan pada sistem keamanan informasi.

   c. *Review* manajemen

Pemantauan organisasi dengan memikirkan keberlanjutan proses bisnis organisasi untuk berjalan lancar sesuai dengan tujuan organisasi dilakukan adanya *review* seperti umpan balik agar mampu melakukan perbaikan, pemantauan, dan pengukuran hasil.

10. Klausa 10 – Peningkatan

    a. Ketidaksesuaian dan tindakan perbaikan

       Organisasi harus memastikan jika terjadi ketidaksesuain pada organisasi dilakukan tindakan perbaikan berkelanjutan agar organisasi selalu mengalami peningkatan dan meningkatkan efektifitas keamanan sistem informasi.

    b. Perbaikan berkelanjutan

       Organisasi perlu melakukan perbaikan secara berkelanjutan agar proses bisnis yang berjalan terus mengalami peningkatan. Perbaikan berkelanjutan dilakukan agar organisasi dapat terus mematuhi standar internasional yang berlaku dan terus melakukan perbaikan untuk meminimalkan risiko yang akan terjadi dikemudian hari.

2.2.6 *Gap Analysis*

Gap analysis merupakan salah satu tindakan dengan memperbandingkan dan melakukan pengidentifikasian terhadap dua data[25]. Gap analysis atau dengan nama lain analisis kesejangan penting diterapkan untuk melihat sampai pada tahap mana perusahaan berada dan berguna sebegai bahan pertimbangan evaluasi kinerja perusahaan [25]. Dengan melakukan gap analysis, perusahaan dapat mengidentifikasi kesenjangan antara kinerja saat ini dan target kinerja yang diharapkan, sehingga dapat merencanakan langkah-langkah konkret untuk mengatasi kesenjangan tersebut.

Variable yang digunakan pada *gap analysis* tertera pada tabel dibawah ini.

Tabel 2. 2 Tabel Variabel Gap Analysis

Skor	Variabel
1	Jika organisasi atau perusahaan tidak mengerti apa yang dibutuhkan dan tidak melakukannya.
2	Jika organisasi atau perusahaan memahami pentingnya aktivitas tetapi tidak melakukannya.
3	Jika organisasi atau perusahaan memiliki dokumen tetapi belum diterapkan atau dilakukan tapi tidak terdokumentasi.
4	Jika organisasi atau perusahaan melakukan aktivitas tetapi tidak konsisten.
5	Jika organisasi atau perusahaan melakukan aktivitas dengan baik (dilakukan secara konsisten).

Tabel variabel gap analysis diterapkan dengan melihat ada pada kondisi skor berapa aktifitas perusahaan. Skor 1 dengan keterangan perusahaan tidak mengerti apa yang dibutuhkan dan tidak melakukannya. Skor 2 dengan keterangan perusahaan memahami pentingnya aktivitas tetapi tidak melakukannya. Skor 3 dengan keterangan perusahaan memiliki dokumen tetapi belum diterapkan atau dilakukan tapi tidak terdokumentasi. Skor 4 dengan keterangan perusahaan melakukan aktivitas tetapi tidak konsisten. Skor 5 dengan keterangan perusahaan melakukan aktivitas dengan baik (dilakukan secara konsisten).

Adapun presentase skor yang digunakan pada *gap analysis* tertera di tabel dibawah ini.

Tabel 2. 3 Tabel Skor Gap Analysis

Skor	Uraian
75%-100%	Organisasi siap untuk mengimplementasikan ISO 27001:2013
50%-74%	Organisasi masih harus berbenah untuk mengimplementasikan
1%-49%	organisasi mendesak adanya perbaikan karena jauh dari persyaratan ISO