BAB II
TINJAUAN PUSTAKA

Tugas akhir ini mengandung referensi dari penelitian Perancangan sebelumnya yang telah dilakukan dengan topik yang sama yaitu ISO 27001. Referensi dilakukan guna mendapatkan perbandingan tentang kelebihan dan kekurangan dari penelitian sebelumnya dan juga untuk menambah wawasan pengetahuan penulis dalam menulis tugas akhir.

2.1 Penelitian Sebelumnya

Berikut tabel hasil penelitian dari jurnal-jurnal yang dilakukan terdahulu.

Tabel 2. 1. Perbandingan penelitian sebelumnya dengan metode ISO 27001

No	Judul	Comparing	Contrasting	Criticize	Synthesize	Summarize
1	International Organization for Standardization (ISO) 3100:2018 dan standar pengendalian menggunakan International Organization for Standardization (ISO) 27001:2013[5].	Melakukan riset ini untuk mengetahui risiko yang ada pada tata kelola dalam perpusnas[5]	Membahas tentang ISO 27001[5]	Hanya membuat informasi tentang risiko[5]	Penelitian ini membuat mengetahuii letak kesalahan sistem[5]	Penelitian ini menunjukan bahwa Audit itu sangat penting.[5]
2	Penilaian Risiko Sistem Informasi Fakultas Teknik	Melakukan penelitian dibidang Audit tata kelola	Membahas tentang Fakultas Teknik Universitas Diponegoro	Melakukan Risk Assesment	Penelitian ini menilai risiko yang ada di dalamnya.	Teknologi informasi sangatlah berpengaruh untuk kemajuan suatu organisasi.

No	Judul	Comparing	Contrasting	Criticize	Synthesize	Summarize
	Universitas Diponegoro Menggunakan Metode Failure Mode Effect And Analysis Berbasis Framework ISO 27001[9].					
3	SNI ISO/IEC 27001 dan Indeks KAMI: Manajemen Risiko PUSDATIN (PUPR)[10].	Melakukan penelitian untuk mengevaluasi Tata Kelola Keamanan Informasi	Membahas tentang SMKI	Tingkat persiapan dan tingkat kesiapan Pusdatin dalam upaya mencapai Sertifikasi ISO 27001:2013.	Penelitian ini mengevaluasi dan Tingkat persiapan dan tingkat kesiapan Pusdatin dalam upaya mencapai sertifikasi ISO 27001:2013.	Pemanfaatan Teknologi Informasi dan Komunikasi (TIK) dalam aktivitas operasional instansi merupakan yang tidak terpisahkan. Semakin tinggi tingkat ketergantungan instansi terhadap TIK, risiko semakin bertambah banyak ancaman situasi yang mungkin terjadi, sehingga perlindungan informasi menjadi sangat penting dan perlu diperhatikan dengan baik.
4	Analisis Manajemen	Menerapkan framework atau	Membahas Penerapan Manajemen Risiko	Adanya sistem dan pemanfaatan teknologi	Enam area praktik keamanan tersebut telah	Berawal dari adanya masalah sebelumnya, belum

No	Judul	Comparing	Contrasting	Criticize	Synthesize	Summarize
	Risiko Keamanan Sistem Informasi pada BKPSDM Kota Batu menggunakan Kerangka Kerja OCTAVE-S dan ISO 27001:2013 (Studi Kasus: Aplikasi E-Kinerja)[11].	kerangka kerja OCTAVES untuk evaluasi risiko yang terkait dan dihubungkan dengan persyaratan pengendalian standar ISO 27001:2013.	keamanan sistem informasi di Badan Kepegawaian, Pendidikan, dan Pelatihan (BKPSDM) Kota Batu.	Informasi memiliki potensi untuk memberikan manfaat positif sebagai alat bantu dalam menjalankan operasional organisasi.	dipilih sebagai fokus untuk dilakukan mitigasi.	ada praktik potensi bahaya dan tidak terdapat dokumen atau kebijakan yang berkaitan dengan keamanan sistem informasi. Tujuan dari penelitian ini adalah untuk mengenali dan memahami secara rinci serta menentukan menyediakan data terkait yang diperlukan.
5	Audit Keamanan Sistem Informasi Manajemen Akademik dan Kemahasiswaan Menggunakan SNI ISO 27001:2013 (Studi Kasus	Melakukan Penelitian dengan SNI ISO 27001:2013	Membahas SNI ISO 27001:2013 STMIK Mardira Indonesia	Hanya dilakukan penelitian Audit Keamanan Sistem Informasi	Melakukan audit pada SIMAK untuk menghasilkan dokumentasi dan mendapatkan bukti audit, serta melakukan evaluasi secara objektif.	Seiring berkembangnya teknologi yang begitu pesat dan cangih memberikan dampak yang signifikan dalam kehidupan saat ini.

No	Judul	Comparing	Contrasting	Criticize	Synthesize	Summarize
	STMIK Mardira Indonesia)[12].					
6	Analisis Dan Penerapan Manajemen Risiko Aplikasi Pemantauan Serta Sistem Manajemen Keamanan Informasi Menggunakan SNI ISO/IEC 27001:2013 (Studi Kasus: KPID Jawa Barat)[13].	Melakukan Penelitian dengan topik dalam bidang keamanan sistem	Membahas tentang SPBE dan SMKI.	Hanya dilakukan penelitian mengunakan SNI ISO/IEC 27001:2013	Diperlukan implementasi manajemen keamanan informasi di lingkungan, khususnya pada sistem monitoring, mengingat adanya data yang merekam konten siaran televisi.	Pengamanan jaringan LAN bertujuan untuk mengurangi risiko sistem monitoring. Diperlukan evaluasi risiko guna memastikan rahasia, integritas, dan ketersediaan informasi, dan juga merancang kontrol untuk mengurangi potensi ancaman yang mungkin terjadi.
7	Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks	Melakukan penelitian dengan katalog Keamanan Informasi	Membahas Desain sistem web untuk *e-Government*	Hanya menggunakan metode penelitian mengunakan pemrograman extreme	Tahapan pengembangan menggunakan Indeks Keamanan Informasi	Sering dengan perkembangan teknologi memasuki semua masyarakat

No	Judul	Comparing	Contrasting	Criticize	Synthesize	Summarize
	Keamanan Informasi (Indeks KAMI) Versi 4.0 pada Dinas Komunikasi dan Informatika Kota Bogor[14].					
8	Risk Management; Risk Assessment of Information Technology Security System at Bank Using ISO 27001[15].	Melakukan penelitian dengan checklist dari Annex A ISO 27001	Untuk mengetahui mana saja yang belum ditangani dengan baik	Membahas aplikasi perbankan	Terdapat pembahasan checklist data	Memastikan bahwa pengendalian yang akan diterapkan memberikan manfaat sebesar-besarnya dengan biaya yang serendah-rendahnya dengan tetap mempertimbangkan tingkat risiko yang akan ada jika tidak dilakukan pengendalian.
9	Analysis of information security issues in corporate	Melakukan penelitian dengan mentode keamanan informasi	Keamanan informasi di jaringan perusahaan	Keamanan jaringan sangat penting bagi perusahaan maupun organisasi.	Pengelolaan jaringan harus bagus	Memastikan keamanan sistem informasi perusahaan merupakan tugas prioritas manajemen perusahaan, karena kecepatan

No	Judul	Comparing	Contrasting	Criticize	Synthesize	Summarize
	computer networks[16].					pengambilan keputusan dan efisiensi perusahaan sangat bergantung pada pelestarian kerahasiaan, integritas, dan ketersediaan aset informasi perusahaan
10	Evaluation of E-Government Maturity Models in Sub-District Public Services in Indonesia Using the SPBE Framework[17].	Melakukan penelitian dengan metode SPBE	Menilai tingkat indeks maturitas dalam pelayanan Pemerintah Daerah	Untuk kedepanya adalah Sosialisasi Portal Pelayanan Publik Kecamatan dilakukan melalui website, leaflet, dan media sosial	Pada hasil akhir yaitu masih membutuhkan audit kembali	Dengan menggunakan aplikasi *e-government* maka harus memberiikan sosialisasi.

Berdasarkan Tabel 2.1 dapat diketahui bahwa perbedan penelitian sebelumnya dengan penelitian yang dilakukan terhadap Keamanan sistem informasi dan *e-governance* terletak pada metode dan tujuan penelitian. Penelitian yang akan dilakukan berupa mengidentifikasikan tingkat risiko tata kelola keamanan informasi. . Hasil penelitian ini memiliki kontribusi meningkatkan hasil assesment.

2.2 Dasar Teori

2.2.1 Manajemen Risiko

Manajemen risiko didefinisikan sebagai keahlian seorang manajer dalam mengatur *fluktuasi* pendapatan dengan mengurangi tingkat kerugian yang terjadi dan disebabkan dengan mempertimbangkan keputusan yang diambil dalam kondisi yang tidak melibatkan kepastian. Prinsip-prinsip dasar dalam manajemen risiko yang dapat dipahami oleh manajemen perusahaan meliputi bahwa manajemen risiko bukan semata-mata metode yang digunakan juga adalah strategi yang dapat diimplementasikan pada berbagai sektor industri [9].

2.2.2 Keamanan Informasi

Menurut penelitian yang dilakukan oleh Sarno dan Iffano (2009), konsep keamanan informasi dapat didefinisikan sebagai proses untuk melindungi data dari berbagai ancaman yang potensial dalam usaha untuk memastikan kelangsungan bisnis, mengurangi potensi risiko yang dihadapi dalam konteks bisnis, dan meningkatkan keuntungan dari pengeluaran modal dampak pada kesempatan bisnis. Contoh yang dapat diambil adalah dari keamanan data. Menurut Sarno dan Iffano (2009), dalam pandangan mereka, meliputi Perlindungan Fisik, Perlindungan Pribadi, Perlindungan Operasi, Perlindungan Komunikasi, dan Perlindungan Jaringan[11].

2.2.3 Indeks Keamanan Informasi (KAMI) tools SMKI

Indeks KAMI adalah sebuah indeks yang instrumen penilaian yang digunakan untuk mengukur tingkat kesiapan dapat dijelaskan sebagai keamanan informasi di instansi pemerintah. Instrumen evaluasi ini dirancang untuk mengevaluasi kematangan atau efektivitas perlindungan yang telah diterapkan, bukan untuk memberikan evaluasi kualitatif atas kondisi persiapan (kecukupan dan kesiapan) kerangka kerja keamanan informasi yang dimiliki pimpinan perusahaan. Evaluasi dilakukan terhadap berbagai aspek yang menjadi fokus penerapan keamanan informasi dengan cakupan pembahasan yang mencakup semua aspek keamanan yang telah ditetapkan oleh standar SNI ISO/IEC 27001[10].

2.2.4 Sistem Pemerintahan Berbasis Elektronik (SPBE)

Sistem Pemerintahan Berbasis Elektronik (SPBE) diartikan sebagai cara pelaksanaan tugas-tugas pemerintahan yang menggunakan teknologi informasi dan komunikasi digunakan untuk menyediakan pelayanan ke para penggunanya. Pengguna Sistem Pemerintahan Berbasis Elektronik (SPBE) meliputi pusat administrasi negara, pemerintahan lokal, karyawan pemerintah, individu, masyarakat umum, pengusaha, dan pihak lain yang menggunakan layanan teknologi informasi dan komunikasi [18].

2.2.5 Sistem informasi

Sistem informasi dapat digambarkan suatu rangkaian data yang menghasilkan informasi yang berguna bagi manajemen. Sistem informasi merupakan suatu sistem yang ada di dalam suatu organisasi, yang memiliki peran penting dalam mengelola dan mengolah informasi secara efektif dan efisien. Sistem informasi yang memenuhi persyaratan pemrosesan transaksi harian yang terjadi, mendukung kegiatan organisasi, serta memiliki sifat strategis, serta memberikan pihak eksternal tertentu dengan laporan yang dibutuhkan[19].

2.2.6 Audit sistem informasi

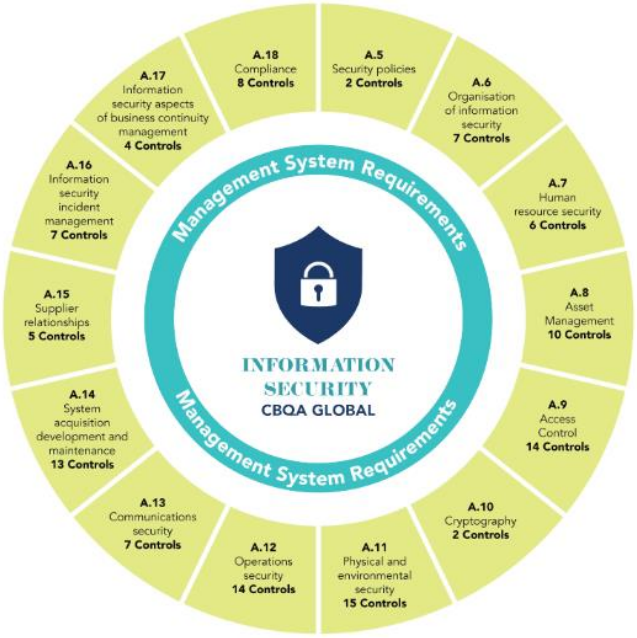
Audit sistem informasi melibatkan pengumpulan dan evaluasi bukti guna mengevaluasi sistem informasi memastikan sistem pengendalian internal telah memadai dan diterapkan melalui sistem penegakan yang terkomputerisasi, semua sumber daya terlindungi beroperasi dengan efektif/tidak disalahgunakan, dan integritas data, keandalan, efektivitas, dan kinerja dalam pengoperasian terkomputerisasi tetap terjaga[20].

2.2.7 ISO 27001:2013

Menurut Sarno (2009), standar ISO/IEC 27001:2013 adalah suatu standar sistem manajemen keamanan informasi yang memberikan panduan secara umum mengenai prosedur perusahaan yang harus dilakukan dalam proses evaluasi, implementasi, dan pengendalian keamanan informasi berdasarkan praktik terbaik dalam pengendalian perlindungan informasi[11].

Standar tersebut mengatur persyaratan yang harus dipenuhi dalam menetapkan, menerapkan, menjaga, dan terus-menerus memperbaiki Sistem Manajemen Keamanan Informasi (SMKI) di suatu perusahaan dan organisasi. Selain itu, memenuhi persyaratan untuk mengevaluasi dan menangani kebutuhan akan keamanan informasi yang

penyesuaian sesuai dengan kebutuhan spesifik organisasi. Kriteria yang harus dipenuhi tercantum di standar SMKI. Pada standar ini memiliki sifat yang bersifat universal dan dapat diadopsi oleh berbagai organisasi, dengan berbagai kategori, dimensi, dan karakteristik. Tidak ada pengecualian yang dapat dibuat terhadap setiap persyaratan yang terdapat dalam Klausul 5 hingga 18 jika organisasi ingin menyatakan kesesuaian dengan standar ini[21].



Gambar 2. 1. Kerangka Keamanan Informasi

ISO 27001 terdiri dari 14 klausul (clause) yang meliputi :

a. A.5 Kebijakan keamanan informasi : Untuk memberikan panduan implementasi dan bantuan manajemen dalam mengimplementasikan pengamanan informasi yang sesuai dengan persyaratan konteks bisnis, regulasi, dan kepatuhan hukum yang berlaku [22].
b. A.6 Organisasi keamanan informasi : Untuk menciptakan struktur manajemen yang memberikan kerangka kerja dalam mengontrol dan memulai pelaksanaan serta pengoperasian keamanan informasi di dalam organisasi [22].
c. A.7 Keamanan sumber daya manusia : Untuk memastikan bahwa staf dan pihak kontrak memiliki pemahaman yang jelas tentang kewajiban mereka dan mematuhi posisi yang telah ditetapkan untuk individu-individu tersebut [22].

d. A. 8 Manajemen aset : Untuk mengenali Harta kekayaan perusahaan dan sumber daya organisasi dan menetapkan Tanggung jawab yang tepat dalam melindungi aset tersebut[22].
e. A. 9 Kendali akses : Mengatur akses dengan batasan yang ditetapkan ke data dan infrastruktur pengolahan data[22].
f. A. 10 Kriptografi : Untuk memastikan penerapan yang tepat dan efektif dalam penggunaan kriptografi dalam menjaga privasi, otentikasi, dan keutuhan informasi [22].
g. A. 11 Keamanan fisik dan lingkungan : Untuk menghindari upaya akses fisik yang tidak sah, kerusakan, atau gangguan terhadap data dan infrastruktur pengolahan data perusahaan [22].
h. A. 12 Keamanan operasi : Agar memastikan bahwa pengoperasian fasilitas pemrosesan informasi dilakukan dengan tepat dan dalam keadaan yang terjamin atau terlindungi [22].
i. A. 13 Keamanan komunikasi : Agar memastikan keamanan data yang berada dalam jaringan dan fasilitas pendukung pengolahan data yang dikumpulkan[22].
j. A. 14 Akuisisi, pengembangan dan perawatan sistem : Agar memastikan keamanan informasi menjadi komponen penting dalam keseluruhan tahapan sistem informasi. Hal ini juga mencakup kebutuhan bagi sistem informasi yang memberikan layanan melalui jaringan publik [22].
k. A. 15 Hubungan pemasok : Untuk menjamin keamanan dan perlindungan dari harta kekayaan organisasi yang mampu dijangkau oleh penyedia[22].
l. A. 16 Manajemen insiden keamanan informasi : Untuk menjamin pendekatan yang seragam dan efisien dalam menajemen kejadian keamanan informasi, termasuk proses komunikasi terkait tentang Peristiwa dan kerentanan keamanan yang terkait[22].
m. A. 17 Aspek keamanan informasi dari manajemen keberlangsungan bisnis : Kontinuitas keamanan informasi harus dijaga dan ditanamkan dalam kerangka manajemen keberlangsungan bisnis perusahaan terkait[22].
n. A. 18 Kesesuaian : Untuk mencegah pelanggaran terhadap ketentuan hukum, peraturan, atau regulasi ketentuan kewajiban kontraktual. Berkaitan dengan perlindungan kebutuhan keamanan informasi dan persyaratan terkait lainnya[22].

Setiap klausul dalam ISO 27001 memiliki persyaratan yang diharuskan terpenuhi oleh organisasi harus memastikan perlindungan informasi yang efektif. Organisasi harus

mengevaluasi dan mengelola risiko keamanan informasi, mengimplementasikan kontrol keamanan yang sesuai, dan secara terus-menerus meningkatkan sistem manajemen keamanan informasi mereka untuk memenuhi persyaratan standar[23].

Dari 14 Klausul diatas peneliti menggunakan, Klausul 6 Organisasi keamanan informasi pada ISO 27001 dikarenakan di klausul tersebut menjelaskan tentang proses risk assessment. Klausul ini menjelaskan bahwa organisasi harus mengevaluasi risiko keamanan informasi yang mungkin timbul dan mengambil tindakan yang sesuai untuk mengelola dan mengurangi risiko tersebut. Klausul ini juga menjelaskan bahwa organisasi harus mengevaluasi risiko secara berkala dan melakukan tindakan yang sesuai digunakan mengatasi risiko yang muncul dari perubahan lingkungan operasional atau perubahan dalam sistem, aplikasi atau data[24].