BAB II

KAJIAN PUSTAKA

Pada bab ini dilakukan pengkajian terhadap penelitian terdahulu dan sumber literatur lainnya, yang menjadi rujukan utama dalam merumuskan masalah penelitian, metode, dan pendekatan yang digunakan.

2.1 Penelitian Terdahulu

Kajian pustaka ini disusun memastikan bahwa konsep-konsep yang diangkat relevan dan mendukung tujuan penelitian secara menyeluruh.

Tabel 1 Rincian penelitian terdahulu

No	Nama Peneliti	Judul	Hasil Penelitian
1	Carol Hsu, Tawei Wang dan Ang Lu	*The Impact of ISO 27001 Certification on Firm Performance*	Penelitian ini bertujuan untuk menguji dampak dan keuntungan didapatkan oleh organisasi setelah mengimplementasikan sertifikasi ISO 27001. Hal ini dikarenakan organisasi membutuhkan cukup banyak biaya untuk dapat mengimplementasikan dan memperoleh sertifikat ISO 27001. Penelitian ini juga membahas ISO 9001 sebagai komparasi terhadap *outcome* yang didapatkan dari implementasi sertifikasi di bidang tersebut. Dimana ISO 9000 yang memiliki fokus terhadap *quality management* atau peningkatan manajemen kualitas memberikan dampak yang lebih jelas ketimbang ISO 27001, yang di perlihatkan

No	Nama Peneliti	Judul	Hasil Penelitian
			dengan peningkatan kualitas produksi dan kepuasan pelanggan. Dilain sisi ISO 27001 tidak menunjukkan hal yang serupa, hal ini dikarenakan fokus ISO 27001 lebih kepada menginisiasikan peran defensif terhadap kemungkinan dampak negatif yang merugikan organisasi. Sehingga pengukuran efektivitas penerapan keamanan informasi akan lebih relevan jika diukur dari kepatuhannya. Kesimpulan penelitian ini adalah ISO 27001 diimplementasikan dengan tujuan untuk memenuhi kewajiban organisasi untuk menjaga keamanan informasi, dan bukan untuk keunggulan kompetitif (Hsu, Wang, & Lu, 2016).
2	Joffre Velasco, Rodrigo Ullauri, Luis Pilicita, Bolívar Jácome, Pablo Saa dan Oswaldo Moscoso-Zea	*Benefits of Implementing an ISMS According to the ISO 27001 Standard in the Ecuadorian Manufacturing Industry*	Penelitian ini membahas mengenai dampak dan/atau manfaat penerapan ISO 27001 di organisasi yang bergerak di bidang manufakturing. Aktivitas sehari-hari yang terjadi di bidang manufaktur membuat perusahaan selalu memproses informasi dalam jumlah yang sangat besar, pada setiap alat elektronik, media fisik dan digital. Dimana kerentanan keamanan informasi dapat terjadi dimana-mana dan jika tidak diatasi, dapat dieksploitasi

No	Nama Peneliti	Judul	Hasil Penelitian
			oleh pihak yang tidak berwenang. Untuk itu organisasi membutuhkan Sistem Manajemen Keamanan Informasi (SMKI) yang diimplementasikan dengan metode *Plan-Do-Check-Act* (PDCA), untuk memastikan *Confidentiality, Integrity dan Availability* (CIA). Standar ISO 27001 digunakan untuk membantu memberikan rekomendasi peningkatan keamanan informasi, dan kerangka kerja MEGRIT II digunakan untuk mengelola risiko. Implementasi SMKI dapat menjadi proses yang rumit dan membutuhkan banyak biaya, namun informasi merupakan aset yang tidak ternilai bagi perusahaan. Dimana ancaman terhadap aset informasi dapat menghentikan bisnis perusahaan dan menyebabkan kerugian yang banyak (Velasco, et al., 2018).
3	Evan Hardyanto Prakasita	Tinjauan Kesiapan Terhadap Implementasi *Business Continuity Management Systems* (BCMS) Berbasis ISO 22301 dan ISO 27001 (Studi Kasus: PT. JPK)	Tesis ini melakukan analisis penilaian kesiapan implementasi BCMS dengan menggunakan ISO 22301 dan ISO 27001. Proses analisis dilakukan dengan menggunakan *self-assessment checklist* dan *in-depth interview* dengan pihak-pihak terkait yang ditentukan dengan metode

No	Nama Peneliti	Judul	Hasil Penelitian
			Responsible, Accountable, Consulted and Informed (RACI), untuk mengisi kuesioner tingkat kesiapan yang pertanyaannya dikumpulkan berdasarkan *best practice* yang dirumuskan oleh ISO 22301 dan ISO 27001. Kemudian merumuskan rekomendasi dan strategi pemenuhan *gap*, berdasarkan hasil analisis yang telah dilakukan (Prakasita, 2018).
4	Purnomo Dwi Djajanto	Rekomendasi Perancangan Sistem Manajemen Keamanan Informasi (SMKI) Menggunakan Metode AHP-TOPSIS Berdasarkan ISO/IEC 27001:2005 (Studi Kasus: PT PJB *Services*)	Dari hasil penelitian yang telah dilakukan, ditemukan sebanyak 224 risiko yang menjadi dasar perancangan Sistem Manajemen Keamanan Informasi (SMKI). Dimana risiko tersebut kemudian dipetakan terhadap kontrol ISO 27001:2005, dan diurutkan berdasarkan tingkat risikonya dengan menggunakan AHP-TOPSIS. Hasil pengukuran tersebut menjadi rekomendasi urutan pembuatan SMKI (Djajanto, 2018).
5	Vaselin Monev	*Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002*	Penelitian ini membahas mengenai penggunaan COBIT 5, untuk digunakan sebagai metode *assessment* atau penilaian terhadap nilai *maturity level* keamanan informasi yang diterapkan di berbagai organisasi. Penilaian dilakukan dengan membuat daftar

No	Nama Peneliti	Judul	Hasil Penelitian
			berdasarkan kontrol-kontrol keamanan yang direkomendasikan oleh ISO 27001:2013. Kemudian dari daftar tersebut dilakukan penilaian melalui peninjauan dokumen dan wawancara. Hasil dari wawancara tersebut kemudian dinilai menggunakan tingkat kematangan yang digunakan oleh COBIT 5 yakni tingkat 0 tidak ada kontrol sama sekali, tingkat 1 kontrol keamanan sudah diterapkan sebagian, namun belum ada dokumentasi, tingkat 2 kontrol keamanan sudah diterapkan seluruhnya, namun masih belum ada dokumentasi, tingkat 3 kontrol keamanan sudah diterapkan secara menyeluruh, dan sudah ada dokumennya, 4 kontrol keamanan sudah diterapkan secara menyeluruh, sudah ada dokumen dan ditinjau secara berkala, 5 kontrol keamanan sudah diterapkan, sudah ada dokumen dan sudah dilakukan peninjauan secara berkala serta dilakukan tindakan perbaikan/peningkatan (Monev, 2020).
6	Misni Harjo Suwito, Shinchi Matsumoto, Junpei	*An Analysis of IT Assessment Security Maturity in Higher*	Penelitian yang dilakukan dalam artikel ini membahas mengenai perancangan penilaian keamanan

No	Nama Peneliti	Judul	Hasil Penelitian
	Kawamoto, Dieter Gollmann dan Kouichi Sakurai	*Education Institution*	informasi dengan menggabungkan *framework* COBIT 4.1, ITIL V3 dan ISO/IEC 27001. Dengan melakukan penggabungan ketiga *framework* ini dinilai dapat membuat penilaian *maturity* penerapan keamanan informasi menjadi lebih efektif. Dimana COBIT mampu mengurangi ancaman kritis yang ada melalui *framework IT governance*-nya, ISO/IEC melalui *framework* Sistem Manajemen Keamanan Informasi memberikan panduan untuk menangani permasalahan keamanan dan ITIL mendukung penerapan keamanan informasi melalui *service management*-nya. Hal ini membuat metode penilaian keamanan informasi ini memberikan hasil yang lebih komprehensif dan efisien (Suwito, Matsumoto, Kawamoto, Gollmann, & Sakurai, 2016).
7	Fotis Kitsios, Elpiniki Chatzidimitriou dan Maria Kamariotou	*The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector*	Keamanan informasi sudah menjadi suatu kebutuhan bagi mayoritas organisasi. Hal ini lah yang dijelaskan dalam penelitian ini, dimana ISO 27001 dinilai mampu menangani risiko yang menjadi ancaman bagi keamanan informasi. Untuk menguji hal tersebut dilakukan *assessment* risiko yang dapat berdampak kepada tiga pilar

No	Nama Peneliti	Judul	Hasil Penelitian
			keamanan informasi yaitu *confidentiality, integrity* dan *availability*. Tingkatan dampak risiko ditentukan dengan menggunakan NIST SP 800-30, yang dijelaskan sebagai berikut *"almost certain", "probable", "possible", "unlikely", or "rare", dimana "almost certain", "probable", and "possible"* adalah risiko yang memiliki kemungkinan untuk terjadi. Penggunaan ISO 27001 dinilai efektif karena menangani risiko dengan menilai, mendokumentasikan dan memastikan untuk selalu diperbarui, mengingat risiko keamanan informasi selalu berkembang dari masa ke masa (Kitsios, Chatzidimitriou, & Kamariotou, 2023).
8	Rosmiati, Imam Riadi dan Yudi Prayudi	*A Maturity Level Framework for Measurement of Information security Performance*	Rekomendasi peningkatan dan/atau perbaikan keamanan informasi yang efektif dapat diterapkan pada organisasi jika sudah mengetahui tingkatan keamanan informasi yang sudah diterapkan di perusahaan terkait. Hal ini lah yang dibahas dalam penelitian ini, dengan menggunakan ISO 27001 tingkat *maturity level* perusahaan XYZ dipetakan untuk mendapatkan

No	Nama Peneliti	Judul	Hasil Penelitian
			rekomendasi yang paling tepat. Metode yang digunakan untuk mengukur tingkat kematangan dalam penelitian ini *Capability Maturity Model* (CMM) untuk *System Security Engineering* (SSE) yang diklasifikasikan ke dalam lima tingkatan yakni, tingkat 0 mengindikasikan tidak ada praktek dasar yang diterapkan, tingkat 1 praktek keamanan informasi sudah diterapkan, tetapi belum didokumentasikan, tingkat 2 praktek sudah direncanakan dan ditinjau, tingkat 3 praktek keamanan informasi sudah dijalankan sesuai dengan yang didefinisikan oleh standar, tingkat 4 praktek keamanan ditingkatkan melalui peninjauan pada setiap prosesnya, tingkat 5 praktek keamanan informasi sudah ditingkatkan secara berkala dan selalu beradaptasi pada perubahan. Hasil penelitian ini menilai bahwa perusahaan XYZ memiliki tingkat keamanan informasi di Level 2, dengan rata-rata tingkat kematangan di setiap klausulnya 2.21, yang berarti masih memiliki gap sebanyak 2.79 untuk mencapai Level 5 (Rosmiati, Riadi, & Yudi, 2016).

Kebaruan dalam tesis ini terletak pada versi standar ISO/IEC 27001 yang digunakan yakni versi tahun 2022, serta objek penelitiannya yaitu aplikasi absensi, dimana hal ini belum dilakukan pada penelitian sebelumnya. Adopsi metode penilaian kematangan *Capability Maturity Model Integration* (CMMI) yang disesuaikan dengan relevansinya terhadap aplikasi absensi. Mengikuti persyaratan yang dikeluarkan oleh *International Accreditation Forum* (IAF), standar yang digunakan adalah ISO/IEC 27001:2022. Dengan begitu rekomendasi yang diusulkan dari hasil evaluasi penilaian penerapan keamanan sistem informasi dalam tesis ini dapat digunakan oleh Dinas Komunikasi Informatika dan Statistik Kabupaten Bandung Barat tanpa harus melakukan transisi dari ISO/IEC 27001:2013.

2.2 Sistem Informasi

Mengutip dari *Britannica*, sistem informasi merupakan sekumpulan komponen yang terintegrasi untuk mengumpulkan, menyimpan dan memproses data serta menyediakan informasi dan pengetahuan (Zwass, 2024). Menurut Kenneth C Laudon dalam bukunya yang berjudul *Management Information Systems: Managing the Digital Firm* edisi 13, sistem informasi dapat didefinisikan sebagai sekumpulan komponen yang saling berkaitan untuk mengumpulkan, mengambil, memproses, menyimpan dan mendistribusikan informasi untuk mendukung pengambilan keputusan dan kontrol dalam organisasi (Laudon & Laudon, 2014). Sementara itu menurut James A. O'Brien dan George M. Marakas dalam bukunya yang berjudul *Management Information Systems* edisi 10, sistem informasi dalam organisasi dapat berupa kombinasi yang terorganisir dari orang, *hardware*, *software*, jaringan komunikasi, sumber data, kebijakan dan prosedur yang menyimpan, mengambil, mengubah dan menyebarkan informasi dalam sebuah organisasi (O'Brien & Marakas, 2011). Sistem informasi merupakan salah satu aset utama bagi mayoritas

organisasi yang ada pada saat ini, atas hal tersebut organisasi harus membuat rencana jangka panjang untuk dapat membantu proses bisnis organisasi tersebut. Peran penting sistem informasi dibantu oleh beberapa komponen vital yang berwujud, tidak berwujud dan yang lainnya bersifat personal. Komponen-komponen ini mengumpulkan, menyimpan dan mendistribusikan data ke seluruh organisasi. Dengan begitu data dikumpulkan dan diolah menjadi informasi untuk kemudian informasi tersebut diubah menjadi pengetahuan organisasi (Bourgeois, Smith, Wong, & Mortati, 2019). Sistem informasi membantu menyimpan dan mendistribusikan informasi untuk mendukung pengambilan keputusan dan kontrol di organisasi. Selain itu, dalam mendukung pengambilan keputusan, koordinasi dan kontrol, sistem informasi dapat membantu *manager* dan pekerja dalam menganalisa masalah, memvisualisasikan masalah yang kompleks dan membuat produk baru.

Sistem informasi merupakan kombinasi dan/atau kumpulan dari informasi-informasi penting yang dibutuhkan oleh organisasi (Laudon & Laudon, 2014). Informasi yang dihasilkan dibentuk kedalam suatu bentuk lain yang berarti dan berguna bagi orang lain. Data sebagai kumpulan fakta yang dibentuk dan muncul di dalam suatu organisasi akan dibentuk menjadi bentuk lain yang lebih mudah dimengerti dan dapat digunakan. Sistem informasi terdiri dari teknologi, organisasi dan manajemen. Selain itu, sistem informasi memiliki komponen *input*, *process* dan *output* yang dipengaruhi oleh organisasi dan lingkungannya.

2.3 Keamanan Informasi

Salah satu tanggung jawab terpenting dari organisasi ketika mengelola informasi adalah menjaga keamanan dan kualitas informasi tersebut. Untuk mendukung hal tersebut organisasi harus memiliki sistem informasi yang dapat memastikan keakuratan, integritas dan keamanannya. Dengan begitu kesalahan,

penipuan dan kerugian keamanan dapat diminimalisir (O'Brien & Marakas, 2011). Untuk memastikan keamanan informasi bagi organisasi bukan hanya sekedar untuk memastikan tiga prinsip keamanan informasi *Confidentiality, Integrity dan Availability* saja, namun keamanan informasi juga bertujuan untuk memberikan manfaat bisnis yang nyata bagi organisasi tersebut (Ashenden, 2008). Penjelasan mengenai CIA dijelaskan pada gambar dibawah ini:

Sumber GitHub

Gambar 1 Confidentiality, Integrity and Availability (CIA)

1. *Confidentiality* (kerahasiaan)

   Kerahasiaan merupakan salah satu dari tiga elemen utama dalam keamanan sistem informasi. Aspek kerahasiaan ini mengharuskan organisasi untuk menjaga dan melindungi informasi dari akses atau pengungkapan yang tidak sah. Untuk itu dibutuhkan pembatasan hak akses kepada pihak yang berwenang.

2. *Integrity* (integritas)

   Aspek integritas berbicara mengenai keutuhan dan keotentikan informasi, dimana untuk itu selama pemrosesan, penyimpanan dan/atau pengelolaan informasi, organisasi harus dapat menjaga akurasi informasi tersebut dari perubahan yang tidak sah.

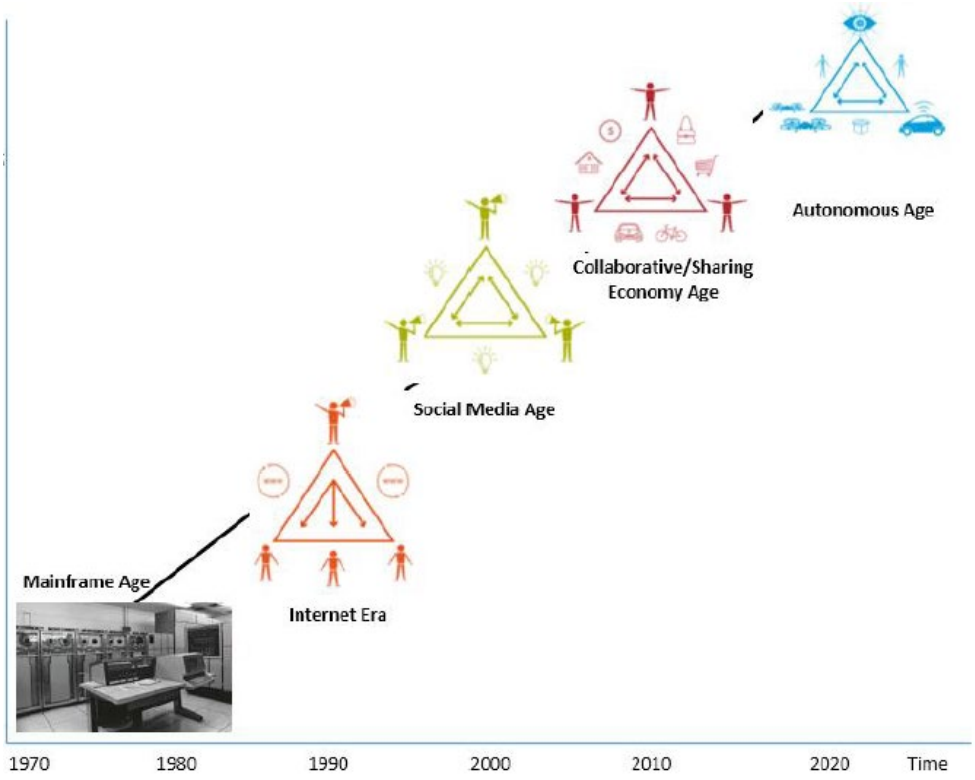
3. *Availability* (ketersediaan)

   Informasi yang tersedia dan dapat diakses kapan saja ketika diperlukan merupakan konsep utama dari aspek ketersediaan. Untuk mencapai hal ini organisasi harus dapat membangun infrastruktur yang dapat mengelola dan menanggapi permintaan informasi kapanpun ketika diperlukan.

   Dengan diterapkannya ketiga aspek keamanan informasi ini dapat membantu organisasi untuk menurunkan risiko terjadinya kegagalan perlindungan informasi (Djajanto, 2018).

2.4 Perlindungan Privasi

Perlindungan terhadap aset informasi dalam organisasi pada masa ini mengalami penambahan konsen, dimana aset informasi bukan lagi sekedar kerahasiaan saja namun sudah berbicara terkait perihal privasi. Menurut penelitian dengan judul artikel *"A Chronological Review of Empirical Research on Personal Information Privacy Concerns: An Analysis of Situational Contexts and Research Constructs"* yang ditulis oleh Haejung Yun, Gwanhoo Lee, Dan J Kim (Yun, Lee, & Kim, 2019), beranggapan bahwa secara konsep perlindungan privasi data pribadi akan dimodifikasi dan diperluas seiring dengan kematangan, kemunculan dan/atau ditemukannya teknologi baru. Sebagai contoh ancaman privasi baru akan muncul ketika pengguna sudah mulai terbiasa menggunakan suatu teknologi dan kemudian mulai menyebarkan informasi data pribadi mereka tanpa sadar karena kebutuhan untuk menggunakan suatu aplikasi dan/atau teknologi yang baru. Berikut fase perkembangan digital menurut Jeremiah Owyang



Sumber: Yun, Lee, & Kim, 2019

Gambar 2 Five Phases of Digital Eras

1. Fase 0, fase ini merupakan fase dimana komputer digital baru dikembangkan dan diperkenalkan, pada masa ini konsep privasi memang bukan merupakan hal yang baru namun konsen akan perlindungan privasi terbatas kepada pemahaman "*right to be alone"*.
2. Fase 1, pada masa ini dengan berkembangnya internet, *World Wide Web* (WWW), dan perdagangan elektronik mulai memantik PIP sebagai hal yang harus diperhatikan. Dimana penggunaan *cookies*, *web beacons* dan perdagangan elektronik yang mulai mengumpulkan data pribadi penggunanya untuk dapat mengetahui kebiasaan belanja mereka. Di era ini pelanggan mulai berfikir hak kepemilikan atas data pribadi mereka, dan mulai melakukan investigasi terkait penggunaan informasi data pribadi.
3. Fase 2, di era ini dengan hadirnya Web 2.0 yang populer dengan konten berbasis user, seperti Blog dan Wiki yang memberikan kemudahan kepada

pengguna internet untuk membagikan informasi apa saja termasuk data pribadinya. Fenomena membuat organisasi untuk lebih mudah menargetkan pelanggannya menggunakan segmentasi dan *data mining*. Hal ini menjadikan konsen PIP di fase ini berfokus pada informasi yang berkaitan dengan perdagangan *online*.

4. Fase 3a, di akhir tahun 2000-an teknologi mendukung konsep ekonomi berbagi dengan menggunakan *Cloud Computing*. Dimana hal ini menimbulkan potensi risiko baru bagi keamanan privasi data pribadi, karena jangkauan informasi dapat melampaui tingkat fisiknya, karena yang sebelumnya data data sensitif akan disimpan secara internal dengan adanya teknologi ini data disimpan dalam bentuk virtual Bersama dengan layanannya. Kemudian dilanjutkan dengan kemunculan *Big Data* karena volume data yang dikumpulkan serta sumber data yang tidak dapat dikendalikan membuat hal ini menjadi rentan terhadap risiko privasi.
5. Fase 3b, kemunculan teknologi otomatis di era ini seperti kendaraan, *Artificial Intelligence* (AI), dan robot pada perangkat pintar membuat pandangan baru terhadap privasi. Karena di era ini organisasi mulai memindahkan aplikasi dan data mereka ke luar lingkungan yang di*hosting* secara eksternal. Situasi ini merupakan salah satu hal yang dapat memunculkan kerentanan baru bagi privasi data pribadi.

Secara umum *General Data Protection Regulation* (GDPR) mendefinisikan data pribadi sebagai informasi yang berkaitan dengan individu tertentu. Sementara itu berdasarkan Undang-undang Nomor 27 tahun 2022 mendefinisikan informasi data pribadi sebagai informasi perseorangan yang dapat diidentifikasi secara langsung maupun tidak langsung, baik dalam bentuk elektronik maupun non-

elektronik (Indonesia, 2022). Berbicara mengenai perlindungan informasi data pribadi, pemahaman mengenai konsep keamanan data pribadi sebagai salah satu dasar dari pemenuhan hak pemilik data, menjadi sangat penting untuk dibahas karena berbagai faktor (Hendrickx, 2022). Selanjutnya Hendrickx menambahkan bahwa, terdapat tiga alasan mengapa perlindungan informasi memerlukan suatu sistem yang sudah tertanam sebagai hak privasi, yakni:

1. Alasan pertama, bahwa privasi dan perlindungan informasi data pribadi merupakan suatu hal yang saling berkaitan antara satu dan lainnya.
2. Alasan kedua adalah karena, privasi merupakan gagasan yang memperkuat dan mendasari konsep perlindungan informasi data pribadi.
3. Alasan terakhir, hak atas privasi dan perlindungan informasi data pribadi merupakan hak yang diakui secara universal sebagai hak asasi manusia.

Pada dasarnya kerentanan privasi data pribadi datang dari keinginan untuk mencapai tujuan tertentu yang sudah ditetapkan sebelumnya, Dimana dalam pelaksanaanya pencapaian tujuan tersebut memerlukan pemrosesan informasi data pribadi. Dalam memproses data pribadi mayoritas pelanggaran privasi terjadi karena kesalahan pengendali (*controller*) dan pengolah (*Processor*) data (Onik, Kim, & Yang, 2019). Fenomena ini dapat dilihat dengan jelas dengan memahami situasi yang terjadi pada saat ini, dimana informasi data pribadi sudah menjadi "nilai tukar" yang wajar digunakan untuk menggunakan suatu layanan yang ditawarkan oleh organisasi penyedia layanan (Choi, Jeon, & Kim, 2019). Kerentanan terhadap privasi data pribadi merupakan suatu fenomena yang umum ditemui, untuk meningkatkan keamanan privasi data pribadi sudah seharusnya untuk memasukkan standar perlindungan privasi ke dalam sistem informasi yang dibangun oleh organisasi. Hal ini dikarenakan pembangunan sistem informasi yang ada saat ini lebih berfokus

kepada keamanan sementara itu tidak dengan privasi. Keadaan ini dapat dijelaskan dengan memahami kontradiksi yang dibawa oleh “data analisis” dan “data privasi”, dimana disatu sisi revolusi peningkatan pengalaman pengguna memiliki permintaan yang sangat tinggi, disisi lain privasi data pribadi tidak dapat diabaikan begitu saja (Onik, Kim, & Yang, 2019).

Hal ini membuat kesadaran perlindungan privasi mulai diperhatikan. Data absensi yang mayoritas merupakan kumpulan dari data privasi menjadi salah konsen utama dalam penulisan tesis ini. Penggunaan standar ISO/IEC 27001 versi terbaru dirasa menjadi hal yang tepat setelah masuknya beberapa kontrol baru terkait perlindungan data privasi.

2.5 Sistem Manajemen Keamanan Informasi

Kemampuan teknologi yang ada di era modern ini tidak hanya sebagai pelengkap dan/atau pendamping bagi manusia untuk mempermudah segala urusannya. termasuk untuk membuat sistem absensi yang efektif di perusahaan atau organisasi. Dengan kemampuannya untuk dapat mengolah informasi yang banyak dengan waktu yang lebih singkat dari metode manual. Untuk mendukung keberlangsungan teknologi informasi dibutuhkan mekanisme atau kerangka kerja yang tepat, salah satu kerangka kerja yang dapat digunakan untuk mendukung teknologi informasi dari sisi keamanan informasi adalah Sistem Manajemen Keamanan Informasi (SMKI). SMKI merupakan suatu kerangka kerja yang membantu perusahaan untuk dapat mengelola keamanan insiden secara menyeluruh (Achmadi, Suryanto, & Ramli, 2018). Mengutip dari Abbass Asosheh et al, SMKI menggunakan persyaratan dan harapan keamanan informasi yang didefinisikan oleh organisasi untuk dijadikan sebagai masukan keamanan informasi (Asosheh, Hajinazari, & Khodkari, 2013). Hal ini membuat penerapan SMKI untuk

meningkatkan keamanan informasi menjadi relevan bagi organisasi, karena SMKI dibangun berdasarkan kebutuhan dan harapan keamanan informasi organisasi itu sendiri.

2.6 ISO/IEC 27001 dan ISO/IEC 27002

Standar ISO/IEC 27001 merupakan standar keamanan informasi yang berada di bawah seri ISO/IEC 27000 (Hamdi, Norman, Molok, & Hassandoust, 2019), dikembangkan dan dipublikasikan oleh *International Organization for Standardization* (ISO) dan *International Electrotechnical Commission* (IEC). Standar ini berdiri dan sejalan dengan kerangka kerja SMKI. Standar ini mulai mengadopsi dan mengembangkan kontrol keamanan informasi berdasarkan SMKI, setelah British Standard mengajukan BS 7799-1 kepada ISO/IEC yang kemudian disetujui dan dipublikasikan sebagai ISO/IEC 17799, yang kemudian berubah menjadi ISO/IEC 27002 pada tahun 2006 (Humphreys, 2011). Sementara itu ISO/IEC 27001 pertama kali dipublikasikan pada tahun 2005, yang berisikan deskripsi dan persyaratan yang harus dipenuhi *Information Security Management System* (ISMS) untuk mendapatkan sertifikasi keamanan informasi (Disterer, 2013). Merujuk kepada standar ISO/IEC 27001 (ISO/IEC, 2022), ISO/IEC 27001 merupakan standar yang menyediakan persyaratan yang dapat digunakan untuk membuat, mengimplementasikan, memelihara dan meningkatkan SMKI. Hal yang sama ditulis oleh (Meriah & Rabai, 2019), bahwa persyaratan keamanan informasi tersebut dipisahkan menjadi 11 kategori, dan 11 kategori tersebut dibagi lagi menjadi beberapa kategori, dengan tujuan untuk memberikan persyaratan keamanan yang detail dan sesuai. Sementara itu, untuk bagaimana cara penerapan persyaratan keamanan informasi tersebut dijelaskan dalam ISO/IEC 27002 (Meriah & Rabai, 2019).

Pada Oktober tahun 2022 lalu, *International Organization for Standardization* (ISO) dan *International Electrotechnical Commission* (IEC) mengevaluasi standar ISO/IEC 27001, dengan mempublish versi terbaru dari seri ISO/IEC 27001 yakni versi 2022. Dimana dalam standar versi terbaru ini terdapat beberapa perubahan minor dan major pada kontrol keamanannya. Kontrol keamanan Annex A memiliki beberapa perubahan minor seperti menggabungkan dua kontrol menjadi satu dan merubah urutan beberapa kontrol yang ada. Beberapa perubahan major juga dilakukan, antara lain dengan menambahkan sebelas kontrol baru, yang dijelaskan pada tabel dibawah ini:

Tabel 2 Kontrol Baru Annex A

Kontrol	**Deskripsi Perubahan/Penambahan**
A.5.7 *Threat intelligence*	Kontrol ini mensyaratkan organisasi untuk dapat mengumpulkan dan menganalisa informasi-informasi yang berkaitan dengan ancaman keamanan informasi. Tujuan utama dari kontrol ini adalah untuk mengantisipasi ancaman tersebut dengan memitigasinya.
A.5.23 *Information security for use of cloud services*	Kontrol ini mensyaratkan organisasi untuk memiliki keamanan *cloud* yang lebih baik, dengan menetapkan standar keamanan untuk layanan *cloud* dan prosedur khusus untuk layanan *cloud*.
A.5.30 *ICT readiness for business continuity*	Kontrol ini mengharuskan organisasi untuk dapat memastikan teknologi informasi dan komunikasi dapat dipulihkan dan/atau digunakan ketika terjadi gangguan.
A.7.4 *Physical security monitoring*	Kontrol ini mengharuskan organisasi

Kontrol	Deskripsi Perubahan/Penambahan
	untuk memantau area-area yang dianggap sensitif seperti (pusat data, produksi dan pengembangan), untuk memastikan hanya pihak yang berwenang yang dapat memasuki area tersebut.
A.8.9 *Configuration Management*	Kontrol ini mengharuskan organisasi untuk dapat mengelola konfigurasi teknologinya, dengan tujuan untuk memastikan bahwa teknologi yang digunakan tetap aman dan terhindar dari perubahan yang tidak sah.
A.8.10 *Information deletion*	Kontrol ini mengharuskan organisasi untuk melakukan penghapusan kepada data-data yang sudah tidak lagi dibutuhkan. Kontrol ini memiliki tujuan untuk menghindari kebocoran data sensitif serta untuk memenuhi persyaratan privasi.
A.8.11 *Data masking*	Kontrol ini mengharuskan organisasi untuk menerapkan mekanisme penyembunyian data (*data masking*), sesuai dengan kebijakan kontrol akses yang sudah ditetapkan oleh organisasi. Tujuan dari kontrol ini adalah untuk melindungi informasi-informasi yang sensitif.
A.8.12 *Data leakage prevention*	Kontrol ini mengharuskan organisasi untuk dapat memiliki dan menerapkan langkah-langkah untuk mencegah terjadinya kebocoran data dan pengungkapan informasi yang sensitif

Kontrol	Deskripsi Perubahan/Penambahan
	dari sistem, jaringan dan perangkat yang digunakan oleh organisasi.
A.8.16 *Monitoring activities*	Kontrol ini mengharuskan organisasi untuk melakukan pemantauan terhadap aktivitas-aktivitas yang tidak wajar dan menerapkan prosedur penanganan insiden yang sesuai.
A.8.23 *Web filtering*	Kontrol ini mengharuskan organisasi untuk memiliki dan mengelola daftar *website* yang dapat diakses, dengan tujuan untuk melindungi sistem organisasi.
A.8.28 *Source coding*	Kontrol ini mensyaratkan organisasi untuk dapat memiliki dan menerapkan prinsip-prinsip pengkodean yang aman dalam proses pengembangan perangkat lunak organisasi. Tujuan kontrol ini adalah untuk mengurangi kerentanan keamanan informasi yang terjadi ketika proses pengembangan perangkat lunak.

Selain itu, penambahan *privacy protection* pada ISO/IEC 27001 versi tahun 2022 dianggap sejalan dengan Undang-undang Nomor 7 Tahun 2022 tentang Perlindungan Data Pribadi (PDP). Dimana hal ini akan sesuai dengan penggunaan aplikasi SMART absensi yang mengelola dan memproses informasi data pribadi pegawainya. Selanjutnya penggunaan ISO/IEC 27001:2022 dalam tesis ini juga didasari oleh persyaratan transisi ISO/IEC 27001:2013 ke ISO/IEC 27001:2022 yang tertera pada *International Accreditation Forum Document Transition Requirements for* ISO/IEC 27001:2022. Dimana transisi ISO/IEC 27001:2022 dijelaskan memiliki masa transisi 3 tahun (36 bulan) sejak dirilisnya ISO/IEC

27001:2022 (International Accreditation Forum, 2023).

2.7 Maturity Level

Tingkatan pengukuran *maturity level* dalam tesis ini mengadaptasi tingkatan kematangan yang didefinisikan oleh *Capability Maturity Model Integration* (CMMI) (CMMI Institute, n.d.), yang dijelaskan pada gambar dibawah ini

Sumber: Tools assessment

Gambar 3 Maturity Level

1. ***Non-existent,*** pada fase ini masih belum ada kesadaran mengenai kebijakan, prosedur dan kontrol keamanan informasi.
2. ***Initial,*** persyaratan keamanan informasi diterapkan secara minimal pada beberapa prosesnya. Pada fase ini proses keamanan informasi belum didokumentasikan dan/atau didefinisikan dengan baik. Tingkat keberhasilan dan/atau penerapan pada setiap prosesnya di fase ini bergantung kepada kemampuan dan/atau kesadaran pegawai yang mengendalikannya.
3. ***Repeatable,*** persyaratan keamanan informasi sudah diterapkan sebagian, belum didukung dengan dokumentasi dan keamanan informasi masih belum dikendalikan melalui *review* berkala. Pada fase ini pegawai masih belum sadar akan tanggung jawabnya masing-masing.
4. ***Defined,*** persyaratan keamanan informasi sudah mulai diterapkan dengan baik dan didukung dengan dokumentasi, serta pegawai sudah menyadari tanggung jawabnya masing-masing. Kekurangan pada fase ini adalah belum adanya program peninjauan secara berkala untuk memastikan efektivitas

penerapan keamanan.

5. ***Managed,*** pada fase ini persyaratan keamanan informasi sudah diterapkan secara menyeluruh dan sudah didukung dengan dokumentasi, serta pegawai sudah menyadari tanggung jawabnya masing-masing. Program peninjauan secara berkala sudah dilakukan dan didokumentasikan. Kekurangan pada fase ini adalah hasil temuan pada proses peninjauan keamanan informasi masih belum ditingkatkan atau dievaluasi.
6. ***Optimized,*** pada fase ini seluruh proses persyaratan keamanan informasi sudah diterapkan dengan baik dan didukung dengan dokumentasi yang lengkap. Pegawai menyadari tanggung jawabnya masing-masing. Keamanan informasi sudah ditinjau secara berkala dan didokumentasikan. Seluruh temuan pada proses peninjauan berkala sudah dievaluasi dan keamanan informasi sudah secara aktif ditingkatkan, sehingga mampu mengatasi semua masalah.

Penggunaan CMMI untuk menilai kematangan memberikan kemudahan bagi organisasi untuk dapat mencapai target kematangan implementasi keamanan informasi (Serrano, Tereso, Ribeiro, & Brito, 2013).