Journal of Information System Research (JOSH)
Volume 4, No. 2, Januari 2023, pp 632−640
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i2.2552

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

Eri Riana, Meiva Eka Sri Sulistyawati*, Octa Pratama Putra

Fakultas Teknologi Informasi, Program Studi Sistem Informasi, Universitas Bina Sarana Informatika, Jakarta
Jl. RS. Fatmawati Raya No.24, RT.7/RW.1, Pd. Labu, Kec. Cilandak, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta, Indonesia
Email: [1]eri.eea@bsi.ac.id, [2,*]meiva.mes@bsi.ac.id, [3]octa.opp@bsi.ac.id
Email Penulis Korespondensi: meiva.mes@bsi.ac.id
Submitted: **18/11/2022**; Accepted: **30/01/2023**; Published: **31/01/2023**

Abstrak−Sudah menjadi kebutuhan saat ini di setiap perusahan mengenai penerapan tata kelola di bidang TIK dalam upaya peningkatan kualitas layanan.Untuk itu maka perlu dilakukan penerapan dan sekaligus melakukan proses audit berkala SMKI pada perusahaan menggunakan standard ISO 27001:2013.Berdasarkan hasil audit dan penelitian ditemukan dalam Annex 7 mempunyai tingkat paling rendah dibandingkan Annex lainnya,karena pada dokumentasi intruksi kerja yang berkaitan dengan labeling belum terdaftar didalam dokumen utamanya sehingga perlu disesuaikan dengan dokumen utamanya.Selain itu, ada dari annex dan klausul lainnya terdapat formulir dan dokumen kurang sesuai antara yang tercantum pada prosedur yang ada dengan judul, sehingga kurang tersinkronisasi.Secara keseluruhan penggunaan ISO 27001:2013 sudah berjalan baik dengan memiliki nilai maturity level 97,45% level 5. Dengan hampir dari seluruh annex dan klausul memenuhi standar dari ISO 27001:2013, sehingga dari hasil penelitian ini diharapkan perusahaan dapat melakukan peningkatan kembali didalam melakukan proses arsip dokumen agar mempermudah dari auditor dalam melakukan audit internal eksternal dan dapat terlaksananya keseluruhan kegiatan sesuai dengan yang ada pada standar ISO 27001:2013.

Kata Kunci: Maturity Level; PDCA**;** Standard ISO 27001:2013; Manajemen Keamanan; Audit Sistem Informasi; Tata Kelola

Abstract−It has become a current requirement in every company regarding the implementation of governance in the ICT field in an effort to improve service quality. For this reason, it is necessary to implement and at the same time carry out an ISMS periodic audit process in companies using the ISO 27001: 2013 standard. Based on the audit and research results found in Annex 7 has the lowest level compared to the other Annexes, because the work instruction documentation related to labeling has not been registered in the main document so it needs to be adjusted to the main document. existing procedures with titles, so they are not synchronized. Overall the use of ISO 27001: 2013 has been going well with a maturity level value of 97.45% level 5. With almost all annexes and clauses meeting the standards of ISO 27001: 2013, so from the results this research It is hoped that the company can make improvements again in carrying out the document archive process so that it makes it easier for the auditor to carry out internal external audits and can carry out all activities in accordance with those in the ISO 27001: 2013 standard.

Keywords: Maturity Level; PDCA; ISO Standard 27001:2013; Security Management; Information System Audit; Governance

1. PENDAHULUAN

Sudah menjadi kebutuhan saat ini di setiap perusahan mengenai penerapan tata kelola [1] di bidang TIK. Oleh sebab itu TIK menjadi bagian yang sangat krusial, pengelolaan tata kelola TIK menjadi bermasalah yang menyangkut ketersediaan (availability), kerahasiaan (confidentiality), dan keutuhan (integrity). PT Indonesia Game merupakan perusahaan game online yang menerapkan system berbasis cloud dalam usaha bisnisnya. Keamanan informasi merupakan aspek yang sangat diperhatikan oleh PT Indonesia Game mengingat game yang dijalankan berbasis online dan cloud. PT Indonesia Game melakukan secara berkala proses audit internal dan eksternal SMKI [2] menggunakan ISO 27001:2013. Dari hasil audit internal dan audit eksternal tersebut memastikan resiko keamanan informasi diterapkan sesuai prosedur standard yang digunakan yaitu ISO 27001:2013 [3]. Proses Audit keamanan sistem informasi [4] adalah suatu cara dalam melakukan pengujian terhadap sistem informasi yang terdapat di dalam organisasi untuk mengetahui apakah sistem informasi yang ada telah sesuai dengan visi, misi dan tujuan organisasi, menguji performa dan untuk mendeteksi resiko dan efek potensial yang mungkin ditimbulkan. SMKI merupakan suatu kegiatan pencegahan terhadap gangguan penyalahgunaan informasi yang dilakukan oleh orang-orang yang tidak bertanggung jawab.

ISO 27001:2013 merupakan kerangka didalam menspesifikasikan kebutuhan untuk pembangunan, penerapan, pengawasan dan peningkatan secara berkala pada pengaturan orang, pengaturan proses dan TIK di sebuah perusahaan hal tersebut bersifat independent dimana manajemen resiko menjadi prasyarat, serta dirancang dalam menjamin agar beberapa pengaturan keamanan yang digunakan dapat melindungi aset informasi dari berbagai risiko dan memberi keyakinan keamanan bagi pemangku kepentingan. Struktur organisasi ISO 27001:2013 [5] dibagi dalam dua besar yaitu :

Journal of Information System Research (JOSH)
Volume 4, No. 2, Januari 2023, pp 632−640
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i2.2552

1. Klausul (mandatory process) merupakan persyaratan yang harus dipenuhi jika organisasi menerapkan SMKI ISO 27001:2013.
2. Annex adalah suatu dokumen yang disediakan serta dijadikan acuan didalam menentukan pengawasan keamanan yang perlu diterapkan di dalam SMKI.

Didalam pelaksanaan tata kelola TIK, faktor keamanan merupakan suatu aspek yang sangat penting untuk diperhatikan untuk menghindari resiko [6] dalam penggunaan TI tersebut, maka PT Indonesia Game melakukan audit internal terhadap Sistem Manajemen Keamanan Informasi (SMKI) menggunakan ISO 27001:2013. Tujuan penelitian jurnal yang dihasilkan pada hasil audit internal menggunakan ISO 27001:2013 yaitu untuk mengetahui tingkat keamanan informasi yang terjadi selama satu tahun dan memberi rekomendasi untuk PT Indonesia Game untuk di lakukan tindakan strategis.

2. METODOLOGI PENELITIAN

2.1 Penelitian Terdahulu

Penelitian yang dilakukan oleh Bakri dan Irmayana [7] dengan judul Keamanan Informasi SIMHP BPKP menggunakan Standar ISO 27001. Penelitian berfokus pada penilaian dan pemetaan permasalahan keamanan terhadap aset informasi pada SIMHP. Berdasarkan penelitian dihasilkan katalog temuan SMKI yang dibuat berdasarkan dari standar Internasional yang diterapkan oleh ISO 27001:2013. Pemetaan dilakukan dengan cara mengidentifikasi artifak keamanan informasi pada SIMHP, melakukan kuisioner dan wawancara oleh Kepala Sub Bagian Prolap dan Administrator SIMHP. Pemodelan SMKI dilakukan dengan mengidentifikasi kendali-kendali keamanan informasi. Selanjutnya proses pelaksanaan audit keamanan sistem informasi dilakukan dengan cara proses pembuatan pembuatan pertanyaan, identifikasi asset informasi, pernyataan, dan penentuan kendali berdasarkan temuan Sistem Manajemen Keamanan Informasi. Penelitian yang dilakukan oleh Sidik, Iriani, dan Yulianto [8] dengan judul jurnal Audit Manajemen Keamanan Teknologi Informasi Menggunakan Standar ISO 27001:2005 Di Perguruan Tinggi XYZ. Standar digunakan framework International Standarization Organization (ISO) 27001: 2005 yang dipilih karena framework dapat di sesuaikan dengan instrumen tempat penelitian tergantung pada kebutuhan organisasi dan difokuskan pada Sistem Manajemen Keamanan Informasi (SMKI). Hasil keseluruhan penelitian JPA = PA1:PA10, NA=JPA/10 menghasilkan nilai akhir rata-rata 65%, menunjukan level positif, namun belum sesuai yang diharapkan oleh perguruan tinggi dimana mengharuskan melakukan evaluasi yang berkesinambungan dan peningkatan control keamanan yang telah direkomendasikan.

Penelitian yang dilakukan oleh Rosmiati dan Riadi [9] dalam penelitiannya berfokus didalam pengukuran keamanan informasi pada XYZ dengan metode analisis maturity model (tingkat kematangan). Penelitiannya bertujuan dalam mengetahui sejauh mana tingkat kematangan dan kesiapan keamanan informasi pada perusahaan XYZ. Hasil pengukurannya dengan metode tingkat kematangan (maturity level) dimana menunjukkan perusahaan XYZ berada di level 2. Untuk itu diberikan suatu rekomendasi untuk bertujuan pada peningkatan keamanan informasi perusahaan.

Penelitian yang dilakukan oleh Heri Wahyudi, Asep Zulianto dan Asep Maulana [10] berdasarkan hasil pengamatan yang ada di SIMAK maka proses pengukuran kinerja yang ditempuh yaitu melalui audit. Supaya proses audit keamanan sistem informasi bisa berjalan dengan sangat baik dibutuhkan standar dalam prosesnya. Secara formal tidak ada acuan baku mengenai standar apa yang akan digunakan atau dipilih oleh Perguruan Tinggi untuk melaksanakan audit keamanan sistem informasi sehingga dapat menggunakan standar sesuai dengan kebutuhan. Penulis melakukan kesimpulan dalam mengaudit SIMAK. Proses Audit merupakan proses kegiatan yang mandiri, terdokumentasi, dan sistematis dalam memperoleh bukti proses audit dan melakukan evaluasi secara objektif sejauh mana kriteria dari proses audit bisa terpenuhi. Metode yang digunakan yaitu metode kualitatif dengan pendekatan studi kasus.Pendekatan studi kasus berguna ketika penelitian bertujuan untuk wawasan teoritis dan empiris yang diteliti. SIMAK dipakai sebagai bagian yang dilakukan penelitian sebab berdasarkan kegiatan utama dari STMIK Mardira Indonesia dan juga menjadi aset informasi yang dipunyai oleh lembaga dalam menghadapi suatu ancaman keamanan atas ketersediaan, kerahasiaan, dan integritas. Data Primer diperoleh melalui hasil wawancara dan tatap muka serta observasi langsung dengan responden. Proses wawancara dilakukan untuk mengambil informasi mengenai kegiatan utama dalam proses kegiatan akademik di STMIK Mardira Indonesia. Dari hasil penelitian teridentifikasi bahwa klausul yang digunakan adalah, annex 5 : Kebijakan Keamanan (Security Policy), annex 7 : Manajemen Aset (Asset Management), annex 9 : Kontrol Akses (Access Control) dan annex 15 : Kepatuhan (Compliance).

Sedangkan Penelitian yang dilakukan oleh Siti Alvi Sholikhatin, Arief Setyanto, Emha Taufiq Luthfi [11] dengan judul jurnal Analisis Keamanan Sistem Informasi Dengan ISO 27001 (Studi Kasus: Sistem Informasi Akademik Universitas Muhammadiyah Purwokerto) bertujuan untuk Mengetahui posisi keamanan informasi yang berjalan pada sistem informasi akademik di Universitas Muhammadiyah Purwokerto dan membantu menyusun kebijakan keamanan informasi dan saran untuk meningkatkan keamanan informasi sesuai dengan standar ISO 27001 dan variabel pendukung. Lain halnya penelitian yang dilakukan oleh Pangky Februari dan Fitria [12] bertujuan untuk mengukur standar keamanan informasi di SMKN Pugung menggunakan ISO 27001. Metodologi

Journal of Information System Research (JOSH)
Volume 4, No. 2, Januari 2023, pp 632−640
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i2.2552

kegiatan penelitiannya adalah audit operasional dimana berkaitan dalam penggunaan secara ekonomis serta efisien atas suatu sumber daya dalam pencapaian sasaran serta tujuan yang diterapkan. Lalu kemudian, hasil di penelitiannya menunjukkan analisis proses penyebaran kuesioner dimana menghasilkan nilai rata-rata 3,32 pada keseluruhan klausul ISO 27001 sehingga sistem keamanan informasi sudah memiliki standar operasional prosedur yang baku dan tertulis. Kemudian, hasil evaluasi dari temuan yang bervariasi di 11 klausul dikategorikan masuk ke dalam level 4 yang berarti di proses bisnis sudah dimonitor serta diukur dengan baik. Dengan itu bisa dikatakan bahwa proses audit SMKI di SMKN 1 Pugung sudah berjalan baik.

Penelitian lain juga dilakukan oleh Fitroh, Muhamad Rizaldi Seputra, Ginanjar Ramadhan, Tania Nur Hafizah Hersyaf, dan Ari Nur Rokhman [13] Tujuan dari penelitiannya ini untuk mengetahui implementasi ISO 27001 dalam bidang manajemen keamanan menggunakan sistematika review. ISO 27001 adalah standarisasi dimana membahas manajemen keamanan sistem informasi. sistematika review metode diterapkan dalam penelitiannya dilakukan ke dalam empat tahap: review identifikasi, penyaringan artikel awal didapatkan sebanyak 24 artikel terkait ISO 27001 dari tahun 2006-2017, lalu kemudian dilakukan kembali filter artikel lebih lanjutnya yaitu filter dengan pemilihan topik manajemen keamanan didapatkan 2 buku dan 3 artikel semenjak dari tahun 2011-2017, dilanjutkan Kembali evaluasi artikel. Hasilnya ditemukan pada masing-masing buku atau artikel bernilai 20%, diantaranya membahas: 1.penerapan ISO 27001 yang bertujuan memastikan pemilihan proses kontrol keamanan yang memadai dalam memberikan kepercayaan kepada stakeholder dan untuk melindungi aset informasi, 2. mengenai proses implementasi standar ISO 27001 dibutuhkan dalam mengesahkan SMKI yang lebih efisien didalam organisasi yang bekerja di dalam sektor transportasi. Organisasi akan didorong oleh sebuah persyaratan untuk mengesahkan SMKI yang Efisien dengan standar ISO 27001, 3. manajemen keamanan yang efektif dengan implementasi ISO 27001, 4. penilaian tentang tender terhadap sektor publik, meningkatkan sektor keamanan dengan penerapan ISO 27001, 5. dalam hal sebagian hasil dari penelitian doktor mengenai SMKI. Dari hasil Penelitian bisa digunakan oleh suatu organisasi yang ingin menerapkan SMKI yang ditetapkan didalam standar ISO 27001, maka di dalam implementasinya ISO 27001 bisa mengidentifikasi peluang-peluang perbaikan serta untuk mengkoordinasikan upaya menujunya sistem kinerja keamanan informasi yang terus berkesinambungan.

Penelitian yang dilakukan oleh Sitta Rif'atul Musyarofah dan Rahadian Bisma [14], pada penelitiannya, pembuatan Strandard Operating Procedure (SOP) didasarkan dalam kebutuhan Dinas Komunikasi dan Informatika Pemerintah kota Madiun. Pembuatan SOP mengacu ke standar keamanan informasi internasional ISO/IEC 37002:2013 dan ISO/IEC 27001:2013 sebagai acuan kontrol keamanan informasi. Pembuatan SOP ini diharapkan bisa mengurangi kerentanan ancaman keamanan informasi dari luar maupun dari dalam perusahaan. Metode yang digunakan yaitu dengan melakukan analisis kesenjangan dengan membandingkan kondisi keamanan Dinas Komunikasi dan Informatika Pemerintah kota Madiun saat ini dengan kondisi sesuai persyaratan ISO/IEC 27001:2013. Penelitian ini memperoleh 19 SOP dan 1 instruksi kerja, serta 29 formulir untuk melengkapi prosedur.

Perbedaan penelitian yang sudah dilakukan oleh peneliti terdahulu dengan yang dilakukan ini adalah pada penelitian ini berfokus mengaudit manajemen keamanan informasi di PT Indonesia Game menggunakan ISO 27001:2013. Dengan kajian ini tentu akan diketahui apakah semua klausul dan annex yang terdapat dalam ISO 27001:2013 sudah di implementasikan dengan baik atau belum dalam satu tahun terakhir. Kemudian selanjutnya diberikan rekomendasi untuk klausul dan annex yang belum terimplementasi dengan prosedur yang ada didalam PT Indonesia Game. Unsur kebaruan dan kontribusi didalam penelitian ini adalah Audit Sistem Manajemen Keamanan Informasi pada perusahaan tersebut menggunakan ISO 27001:2013 [15]. Oleh karena itu, dengan penelitian ini diharapkan dapat memberikan kontribusi berupa rekomendasi-rekomendasi berdasarkan standar ISO 27001:2013.

2.2 Metode Penelitian

Berikut ini disajikan bahan kajian, metode penelitian yang dipergunakan dan tahapan penelitian yang dilakukan.

2.2.1 ISO 27001:2013

Standard ISO 27001:2013 merupakan suatu revisi dari standard sebelumnya yaitu standard ISO 27001:2005. ISO 27001:2013 tetap bisa diadopsi oleh suatu organisasi sebagaimana versi-versi yang terdahulu. Sistem Manajemen Keamanan Informasi ISO 27001:2013 telah ditetapkan oleh Badan Standarisasi Nasional Nomor 61/KEP/BSN/4/2016 serta Peraturan Menteri Kominfo Nomor 4 tahun 2016 Pasal 7. Dalam ISO 27001:2013 terdapat 14 area pengamanan informasi yaitu kebijakan keamanan informasi, keamanan sumber daya manusia, manajemen asset, mengakses kontrol dan mengelola akses pengguna, teknologi kriptografi, keamanan fisik, keamanan operasional, mengamankan komunikasi dan transfer data, kkuisisi, pengembangan, dan dukungan sistem informasi yang aman, keamanan untuk pemasok dan pihak ketiga, manajemen Insiden, kesinambungan bisnis/pemulihan bencana, dan kepatuhan.

2.2.2 Keamanan Informasi

Keamanan Informasi adalah suatu proses penjagaan informasi dari keseluruhan ancaman yang mungkin bisa saja terjadi dalam upaya untuk memastikan dan menjamin kelangsungan bisnis, meminimalisasi resiko bisnis serta

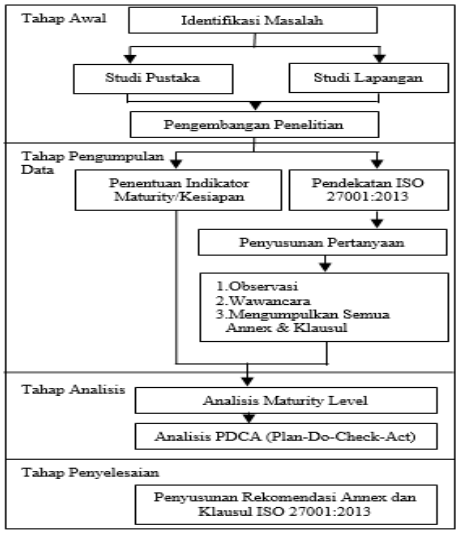
Journal of Information System Research (JOSH)
Volume 4, No. 2, Januari 2023, pp 632−640
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i2.2552

memaksimalkan ataupun mempercepat pengembalian investasi serta peluang bisnis. Keamanan sistem informasi merupakan suatu bentuk kegiatan perlindungan atau pencegahan terhadap gangguan penyalahgunaan informasi yang dilakukan oleh orang yang tidak bertanggung jawab terhadap jalannya suatu sistem [16]

2.2.3 Audit Sistem Informasi

Audit sistem informasi adalah suatu cara melakukan pengujian terhadap sistem informasi yang terdapat dalam suatu perusahaan untuk mengetahui apakah suatu sistem informasi yang dimiliki telah sesuai dengan misi, visi dan tujuan perusahaan, menguji performa sistem informasi serta untuk mendeteksi risiko dan efek potensial yang mungkin ditimbulkan dikemudian hari [17].

Metode penelitian didalam penulisan ini menggunakan metode penelitian campuran antara penelitian kuantitatif dan kualitatif, dimana metode penelitian ini dilakukan dengan cara mengkombinasikan antara dua metode penelitian sekaligus yaitu kuantitatif dan kualitatif dalam suatu penelitian sehingga didapatkan hasil yang lebih valid, reliabel komprehensif, dan objektif. Didalam penelitian jurnal ini, peneliti merancang sebuah kerangka metodologi yang dipergunakan sebagai dasar dari tahapan penelitian sebagaimana yang digambarkan pada gambar 1 berikut ini.



Gambar 1. Tahapan Penelitian

Penelitian dimulai dengan melakukan identifikasi masalah, metode pengumpulan data yang dilakukan dalam penelitian jurnal ini dengan mengumpulkan data primer dimana data primer data yang berasal dari sumber asli atau pertama. data primer pada penelitian jurnal ini diperoleh melalui pengamatan langsung (observasi) yang meliputi data gambaran dari hasil observasi yang dilakukan self-assessment menggunakan klausul standar ISO 27001:2013. Standar ISO 27001:2013 menggunakan project check list untuk mengukur tingkat keamanan informasi sebuah organisasi dengan klausul-klausul yang berbeda di setiap tahapan siklus PDCA. Adapun tahapan penelitian dilakukan dengan merujuk pada siklus PDCA (Plan-Do-CheckAct) [18]. Selain itu juga dilakukan wawancara dengan Kepala Bidang Tata Kelola Teknologi Informasi dan Komunikasi dan Staff Dept terkait. Melakukan dokumentasi dengan cara mencari dan mengumpulkan evidence untuk melihat semua Annex dan Klausul telah diimplementasikan berdasarkan buku ISO 27001:2013.

Setelah itu dilakukan tahapan analisis dengan mengukur tingkat kematangan (maturity level) untuk mengetahui bagaimana selama ini organisasi tersebut mengimplementasikan klausul dan annex pada ISO 27001:2013. Instrumen pengukuran maturity level yang digunakan dijelaskan pada Tabel 1.

Tabel 1. Skala Maturity level

Level	Skala Index Maturity	Deskripsi
0 - Non Existent	0% - 18%	Belum adanya permasalahan yang harus diatasi.Perusahaan merasa tidak membutuhkan mekanisme proses keamanan . Sehingga tidak ada pengawasan sama sekali.
1 - Initial/ Ad Hoc	19% - 36%	Sudah adanya bukti bahwa perusahaan mengetahui adanya permasalahan yang harus diatasi. Perusahaan sudah memiliki inisiatif untuk melakukan keamanan. Namun sifatnya masih non formal.
2 - Repeatable but Intuitive	37% - 54%	Sudah adanya perencanaan, pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Perusahaan memiliki kebiasaan

Journal of Information System Research (JOSH)
Volume 4, No. 2, Januari 2023, pp 632−640
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i2.2552

Level	Skala Index Maturity	Deskripsi
		terpola untuk merencanakan keamanan yang dilakukan secara berulang namun belum melibatkan dokumen formal.
3 - Defined	56% - 72%	Sudah memiliki proses keamanan yang sudah didokumentasikan dengan baik kemudian dikomunikasikan melalui pelatihan. Perusahaan juga menyadari perlunya proses keamanan sehingga adanya aturan yang menunjukkan untuk perusahaan secara rutin melakukan keamanan
4 - Managed and Measurable	73% - 90%	Sudah adanya proses komputerisasi dengan baik, pengembangan sistem sudah terarah dan dijalankan secara terorganisir. Proses keamanan sudah secara formal dilakukan dan secara terus menerus dievaluasi untuk meningkatkan layanan perusahaan.
5- Optimised	91% - 100%	Sudah mengikuti best practice yang ditandai dengan adanya proses otomatisasi pada sistem dengan metodologi yang tepat.

Untuk mengetahui tingkat kematangan (Maturity Level) Klausul dan Annex menggunakan rumus maturity level pada (1).

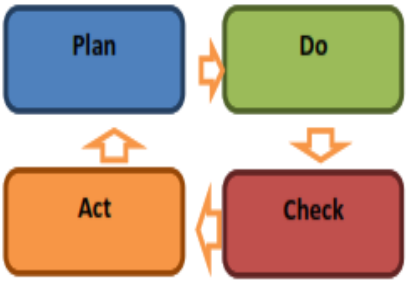
$$\text{Index Maturity} = \frac{Jumlah\ pertanyaan\ yang\ dijawab}{Jumlah\ pertanyaan\ klausan\ dan\ annex} * 100 \quad (1)$$

Pada rumus (1) menjelaskan tentang cara mengetahui tingkat kematangan Klausal dan Annex, yaitu dengan cara menghitung jumlah pertanyaan yang dijawab oleh responden dikalikan dengan bobot setiap jawaban yang telah ditentukan kemudian dibagi dengan total pertanyaan. Pilihan jawaban yang diajukan menggunakan skala likert sebanyak 6 jawaban yang mewakili maturity level (level 0-5). Dilanjutkan tahapan analisis mengenai PDCA (Plan-Do-CheckAct), Adapun gambaran tahapan PDCA dijelaskan dalam table 2 berikut ini :

Tabel 2. Tahapan Siklus Plan-Do-Check-Act (PDCA)

Tahapan Siklus	Keterangan
Plan (membangun SMKI)	Menyusun kebijakan SMKI, objektif, proses dan prosedur yang sesuai untuk pengelolaan risiko dan meningkatkan keamanan informasi untuk memberikan hasil yang sesuai dengan kebijakan organisasi secara keseluruhan.
Do (implementasi dan operasi SMKI)	Implementasi dan menjalankan kebijakan, kontrol, proses dan prosedur SMKI.
Check (memonitor dan me- review SMKI)	Mengukur kinerja proses yang tidak sesuai dengan kebijakan, objek dan laporan praktis SMKI untuk menghasilkan review manajemen.
Act (menjaga dan meningkatkan SMKI)	Mengambil langkah preventif dan korektif berdasarkan hasil audit internal SMKI dan review manajemen atau informasi lain yang relevan, untuk meningkatkan SMKI yang terus berkelanjutan.

Siklus PDCA sendiri terdiri dari aktivitas: membangun, mengimplementasi, mengoperasikan, memonitor, me-review, merawat dan meningkatkan SMKI secara terdokumentasi dalam konteks aktifitas bisnis perusahaan dan risiko yang dihadapi.



Gambar 2. Diagram Siklus PDCA

Journal of Information System Research (JOSH)
Volume 4, No. 2, Januari 2023, pp 632−640
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i2.2552

3. HASIL DAN PEMBAHASAN

3.1 Analisis Maturity Level

Hasil dari maturity level pada PT Indonesia Game berdasarkan analisis dokumen, wawancara, dan observasi dengan checklist sesuai dengan ISO 27001:2013. Hasil analisis maturity level [19] dapat dilihat pada Tabel 3.

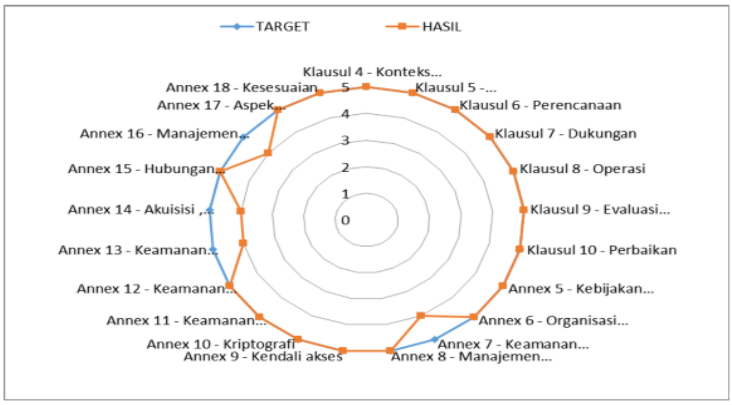
Tabel 3. Hasil Analisis Maturity Level

Klausul Dan Annex	Target	Hasil
Klausul 4 - Konteks Organisasi	5	5 (100%)
Klausul 5 – Kepemimpinan	5	5 (100%)
Klausul 6 - Perencanaan	5	5 (94,42%)
Klausul 7 - Dukungan	5	5 (100%)
Klausul 8 – Operasi	5	5 (100%)
Klausul 9 - Evaluasi Kinerja	5	5 (100%)
Klausul 10 - Perbaikan	5	5 (100%)
Annex 5 - Kebijakan Keamanan Informasi	5	5 (100%)
Annex 6 - Organisasi keamanan informasi	5	5 (100%)
Annex 7 - Keamanan sumber daya manusia	5	4 (84,44%)
Annex 8 - Manajemen aset	5	5 (92,68%)
Annex 9 - Kendali akses	5	5 (100%)
Annex 10 - Kriptografi	5	5 (100%)
Annex 11 - Keamanan fisik dan lingkungan	5	5 (100%)
Annex 12 - Keamanan operasi	5	5 (100%)
Annex 13 - Keamanan komunikasi	5	4 (86,81%)
Annex 14 - Akuisisi , pengembangan dan perawatan sistem	5	4 (88,50%)
Annex 15 - Hubungan Pemasok	5	5 (100%)
Annex 16 - Manajemen insiden keamanan informasi	5	4 (86,81%)
Annex 17 - Aspek keamanan informasi dari manajemen keberlangsungan bisnis	5	5 (100%)
Annex 18 - Kesesuaian	5	5 (100%)
Total Maturity Level		**97,45%**

Pada Table 3 hasil dari analisis tingkat maturity level menggunakan perhitungan persen (%). Klausul 4 mendapatkan hasil 100% berada pada level 5 yaitu Optimised artinya pada klausul sudah berjalan sesuai standar ISO 27001:2013 dan dokumentasi audit sudah lengkap. Pada Klausul 5 mendapatkan hasil 100% berada pada level 5 yaitu Optimised artinya klausul ini sudah berjalan sesuai standar ISO 27001:2013 dan dokumentasi audit sudah lengkap. Pada Klausul 6 hasil 94,42% berada di level 5 yaitu Optimised artinya pada klausul sudah berjalan sesuai standar ISO 27001:2013 dan dokumentasi audit sudah cukup lengkap namun pedoman perlu di revisi di bagian tabel deskripsi karena tidak adanya kolom risk owner dan diharapkan di sesuaikan dengan dokumen risk register. Pada Klausul 7 didapatkan hasil 100% pada level 5 yaitu Optimised artinya pada klausul sudah berjalan sesuai standar ISO 27001:2013 dan dokumentasi audit sudah lengkap. Pada Klausul 8 mendapatkan hasil 100% pada level 5 yaitu Optimised artinya pada klausul sudah berjalan sesuai standar ISO 27001:2013 dan dokumentasi audit sudah lengkap. Pada Klausul 9 didapatkan hasil 100% berada di level 5 yaitu Optimised artinya pada klausul sudah berjalan sesuai standar ISO 27001:2013 dan dokumentasi audit sudah cukup lengkap namun di klausul dokumen pemantauan dan pengukuran belum ada. Pada Klausul 10 hasil 100% berada pada level 5 yaitu Optimised yang artinya pada klausul sudah berjalan sesuai sandar ISO 27001:2013 dan dokumentasi audit sudah lengkap. Pada Annex 5 mendapatkan hasil 100% berada pada level 5 yaitu Optimised artinya pada annex ini sudah berjalan sesuai dengan standar ISO 27001:2013 dan dokumentasi audit sudah lengkap. Pada Annex 6 mendapatkan hasil 100% di level 5 yaitu Optimised yang artinya pada annex ini sudah berjalan sesuai dengan standar ISO 27001:2013 dan dokumentasi untuk audit sudah lengkap. Pada Annex 7 mendapatkan hasil 100% berada pada level 4 yaitu Managed and Measurableyang artinya pada annex ini sudah berjalan sesuai dengan standar ISO 27001:2013 dan dokumentasi untuk audit perlu di cek kembali dalam dokumen kontrak terkait item tanggung jawab keamanan informasi. Pada Annex 8 mendapatkan hasil 92,68% berada pada level 5 yaitu Optimised yang artinya pada annex ini sudah berjalan sesuai dengan standar ISO 27001:2013 dan dokumentasi untuk audit perlu di cek kembali terkait prosedur pelebelan informasi. Pada annex 9 mendapatkan hasil 100% berada pada level 5 yaitu Optimised yang artinya pada annex ini sudah berjalan sesuai dengan standar ISO 27001:2013 dan dokumentasi untuk audit sudah lengkap. Pada annex 10 mendapatkan hasil 100% berada pada level 5 yaitu Optimised yang artinya pada annex ini sudah berjalan sesuai dengan standar ISO 27001:2013 dan dokumentasi untuk audit sudah lengkap. Pada annex 11 mendapatkan hasil 100% berada pada level 5 yaitu Optimised yang artinya pada annex ini sudah berjalan sesuai dengan standar ISO 27001:2013 namun perlu disediakan lokasi bongkar muat dan dokumentasi untuk audit sudah lengkap. Pada annex 12 mendapatkan hasil

Journal of Information System Research (JOSH)
Volume 4, No. 2, Januari 2023, pp 632−640
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i2.2552

100% berada pada level 5 Optimised yang artinya pada annex ini sudah berjalan sesuai dengan standar ISO 27001:2013 dan dokumentasi sudah lengkap. Pada annex 13 mendapatkan hasil 86,81 berada pada level 4 yaitu Managed and Measurable yang artinya pada annex ini sudah berjalan sesuai dengan standar ISO 27001:2013 dan dokumentasi untuk proses audit sudah lengkap. Pada Annex 14 mendapatkan hasil 88,50% berada pada level 4 yaitu Managed and Measurable yang artinya pada annex ini sudah berjalan sesuai dengan standar ISO 27001:2013 dan dokumentasi untuk proses audit sudah cukup lengkap. Pada annex 15 mendapatkan hasil 100% berada pada level 5 yaitu Optimised yang artinya pada annex ini sudah berjalan sesuai dengan standar ISO 27001:2013 dan dokumentasi untuk audit sudah lengkap. Pada annex 16 mendapatkan hasil 85,71% berada pada level 4 yaitu Managed and Measurable yang artinya pada annex ini sudah berjalan sesuai dengan standar ISO 27001:2013 dan dokumentasi sudah cukup lengkap. Pada annex 17 mendapatkan hasil 100% berada pada level 5 yaitu Optimised yang artinya pada annex ini sudah berjalan sesuai dengan standar ISO 27001:2013 dan dokumentasi untuk audit sudah lengkap. Terakhir annex 18 mendapatkan hasil 100% berada pada level 5 yaitu Optimised yang artinya pada annex ini sudah berjalan sesuai dengan standar ISO 27001:2013 dan dokumentasi untuk audit sudah lengkap. Dapat dilihat bahwa pada Annex 7 memiliki hasil paling rendah yaitu 84,44%. Karena kurangnya dokumen sebagai bukti dari annex tersebut membuat annex tersebut memiliki tingkat kematangan (maturity level) yang rendah. Hasil rata-rata dari tingkat kematangan ISO 27001:2013 pada PT Indonesia Game adalah 97,45% dengan level 5 Optimised . Secara keseluruhan ISO 27001:2013 dokumentasi telah dilaksanakan dengan baik hanya perlu ditingkatkan dan dilengkapi kembali mengenai pengarsipan. Spider chart semua klausul dan annex setelah dianalisis dapat dilihat pada gambar 3.



Gambar 3. Spider Chart Maturity Level Klausul dan Annex PT Indonesia Game

3.2 Analisis PDCA (Plan-Do-Check-Act)

Observasi dan Assessment dilakukan menggunakan project list sesuai standar ISO 27001:2013 dan fase pada model PDCA (Plan-Do-Check-Act) [20], Pada fase Plan (membangun SMKI), kegiatan yang dilakukan antara lain:

a. Penentuan scope serta batasan Sistem Manajemen Keamanan Informasi dalam sebuah karakteristik organisasi, bisnis, asset, lokasi dan teknologi.
b. Menentukan kebijakan SMKI.
c. Mengidentifikasi risiko.
d. Menganalisis dan mengevaluasi risiko.
e. Mengidentifikasi dan mengevaluasi opsi untuk menangani risiko.

Selanjutnya, pada fase kedua yaitu Do (implementasi dan operasi SMKI), aktivitas- aktivitas yang dilakukan:

a. Mengelola operasi SMKI.
b. Mengelola sumber daya SMKI.
c. Mengimplementasikan prosedur dan kontrol lain yang bisa mendeteksi keamanan dan merespon ancaman terhadap keamanan.
d. Memformulasikan rencana penanganan risiko yang mengidentifikasi langkah manajemen yang sesuai, sumber daya, tanggung jawab dan prioritas untuk mengelola risiko keamanan informasi.
e. Mengimplementasi rencana penanganan risiko untuk mendapatkan objek kontrol yang teridentifikasi, termasuk rencana anggaran dan alokasi peran serta tanggung jawab.

Proses ketiga yaitu Check meliputi:

a. Melakukan monitor dan mengecek ulang keseluruhan prosedur serta kontrol.
b. Proses review secara rutin mengenai efektifitas Sistem Manajemen Keamanan Informasi.
c. Mengadakan audit internal SMKI.
d. Memperbarui rencana keamanan.

Journal of Information System Research (JOSH)
Volume 4, No. 2, Januari 2023, pp 632−640
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i2.2552

e. Merekam aksi dan kegiatan yang dimungkinkan berimbas pada efektifitas kinerja SMKI

Proses fase terakhir didalam siklus PDCA yaitu Act yaitu :

a. Menerapkan proses peningkatan SMKI.
b. Menjalankan proses tindakan preventif dan korektif yang sesuai.
c. Mengkomunikasikan setiap adanya tindakan dan improvements kepada keseluruhan departemen terkait.
d. Memastikan bahwa semua peningkatan telah berjalan sesuai dengan objek yang teridentifikasi

4. KESIMPULAN

Berdasarkan hasil audit internal dengan acuan standar ISO 27001:2013 pada PT Indonesia Game menggunakan perhitungan maturrity level, Annex 7 memiliki tingakatan paling rendah diantara Annex lainnya disebabkan pada dokumen intruksi kerja terkait labeling tidak terdaftar dalam dokumen utamanya sehingga perlu disesuaikan kembali dokumen utamanya. Selain itu, masih ada dari klausul dan annex lainnya masih terdapat beberapa dokumen dan formulir yang kurang sesuai antara kebijakan/prosedur yang tercantum dengan judul yang ada sehingga kurang adanya sinkronisasi. Namun secara keseluruhan penggunaan ISO 27001:2013 telah terlaksana dengan baik karena memiliki rata-rata 97,45% dengan level 5 Optimised. Hampir dari seluruh klausul dan annex memenuhi standar ISO 27001:2013 terlaksana sehingga dari hasil penelitian ini diharapkan PT Indonesia Game dapat meningkatkan kembali dalam arsip dokumen agar memudahkan auditor dalam melakukan proses audit internal ataupun proses audit eksternal serta dapat terlaksananya seluruh kegiatan sesuai dengan standar ISO 27001:2013.

REFERENCES

[1] D. Rutanaji, S. S. Kusumawardani, and W. W. Winarno, “ISO 27001 sebagai Metode Alternatif bagi Perancangan Tata Kelola Keamanan Informasi (Sebuah Usulan untuk Diterapkan di Arsip Nasional RI),” Pros. Semin. Nas. ReTII ke-12 2017, pp. 168–173, 2017, [Online]. Available: https://journal.itny.ac.id/index.php/ReTII/article/view/604.

[2] W. Apriandari and A. Sasongko, “Analisis Sistem Manajemen Keamanan Informasi Menggunakan Sni Iso / Iec 27001 : 2013 Pada Pemerintahan Daerah Kota Sukabumi (Studi Kasus : Di Diskominfo Kota Sukabumi),” Ilm. SANTIKA, vol. 8, no. 1, pp. 715–729, 2018.

[3] H. Jauhary, G. E. Pratiwi2, A. Z. Salim, and F. Fitroh, “Penerapan ISO27001 dalam Menjaga dan Meminimalisir Risiko Keamanan Informasi : Literatur Review,” Media J. Inform., vol. 14, no. 1, p. 43, 2022, doi: 10.35194/mji.v14i1.1581.

[4] D. Y. Putra, T. Wati, and I. W. Widi P, “Audit Keamanan Sistem Informasi Berdasarkan Sni - Iso 27001 Pada Sistem Informasi Akademik Universitas Pembangunan Nasional ‘Veteran’ Jakarta,” Semin. Nas. Pengaplikasian Telemat. (SINAPTIKA 2020), no. Sinaptika, pp. 1–18, 2020.

[5] Erfina, E. Utami, and A. Sunyoto, “Evaluasi Tingkat Kematangan Keamanan Informasi Pada Sistem Iinformasi Manajemen Universitas Cokroaminoto Palopo,” J. Ilm. d’Computare, vol. 8, p. 50, 2018.

[6] I. Santosa and D. Kuswanto, “Analisa Manajemen Resiko Keamanan Informasi pada Kantor Pelayanan Pajak Pratama XYZ,” Rekayasa, vol. 9, no. 2, p. 108, 2016, doi: 10.21107/rekayasa.v9i2.3347.

[7] M. Bakri and N. Irmayana, “Analisis Dan Penerapan Sistem Manajemen Keamanan Informasi Simhp Bpkp Menggunakan Standar Iso 27001,” J. Tekno Kompak, vol. 11, no. 2, p. 41, 2017, doi: 10.33365/jtk.v11i2.162.

[8] M. Sidik, A. Iriani, and S. Yulianto, “Audit Manajemen Keamanan Teknologi Informasi Menggunakan Standar Iso 27001 : 2005 Di Perguruan Tinggi Xyz,” J. SITECH Sist. Inf. dan Teknol., vol. 1, no. 2, pp. 73–82, 2018, doi: 10.24176/sitech.v1i2.2564.

[9] I. Riadi, “Analisis Keamanan Informasi Berdasarkan Kebutuhan Teknikal Dan Operasional Mengkombinasikan Standar ISO 27001 : 2005 Dengan Maturity Level (Studi Kasus Kantor Biro Teknologi Informasi PT . XYZ),” Semin. Nas. Teknol. Inf. Dan Multimed. 2016, vol. 4, no. 1, pp. 1–2, 2016.

[10] H. Wahyudi, A. Zulianto, and A. Maulana, “AUDIT KEAMANAN SISTEM INFORMASI MANAJEMEN AKADEMIK DAN KEMAHASISWAAN MENGGUNAKAN SNI ISO/IEC 27001 : 2013 (Studi Kasus STMIK Mardira Indonesia),” J. Comput. Bisnis, vol. 14, no. 1, pp. 40–46, 2020.

[11] S. A. Sholikhatin, A. Setyanto, and E. T. Luthfi, “Analisis Keamanan Sistem Informasi Dengan ISO 27001 (Studi Kasus: Sistem Informasi Akademik Universitas Muhammadiyah Purwokerto),” J. Ilm. IT CIDA, vol. 4, no. 1, pp. 1–9, 2019, doi: 10.55635/jic.v4i1.75.

[12] P. Februari and F. Fitria, “Audit Sistem Keamanan Informasi Menggunakan ISO 27001 pada SMKN 1 Pugung, Lampung,” POSITIF J. Sist. dan Teknol. Inf., vol. 5, no. 2, p. 97, 2019, doi: 10.31961/positif.v5i2.833.

[13] A. N. R. Fitroh, Muhamad Rizaldi Seputra, Ginanjar Ramadhan, Tania Nur Hafizah Hersyaf, “Pentingnya Implementasi Iso 27001 Dalam Manajemen Keamanan : Sistematika Review,” Semin. Nas. Sains dan Teknol. 2017, no. November, pp. 1–2, 2017.

[14] S. Rif and R. Bisma, “Pembuatan Standard Operating Procedure (SOP) Keamanan Informasi Berdasarkan Framework ISO / IEC 27001 : 2013 dan ISO / IEC 27002 : 2013 pada Dinas Komunikasi dan Informatika Pemerintah Kota Madiun,” JEISBI Vol. 01 Nomor 01, 2020 (Journal Emerg. Inf. Syst. Bus. Intell. Pembuatan, vol. 01, pp. 43–50, 2020.

[15] I. Yustiana, “Perancangan Tata Kelola Keamanan Informasi Menggunakan Kerangka Kerja Cobit 5,” pp. 1–9, 2017.

[16] Suharjanti, “Prosiding Seminar Nasional Aplikasi Sains & Teknologi (SNAST) 2014 Yogyakarta, 15 November 2014 ISSN: 1979-911X,” Snast, no. November, pp. 211–216, 2014.

[17] T. Ramdhany and M. Asikin, “Audit Sistem Informasi Aplikasi Starclick Menggunakan Framework Cobit 4.1 Domain Deliver and Support Di Pt. Telekomunikasi Regional Iii Jawa Barat,” J. Komput. Bisnis, vol. 11, no. 1, pp. 33–39, 2018.

[18] S. T. Yuwono, N. Pratama, and V. Afifah, “Re-Assessment Konsistensi Dokumen Kontrol Sertifikasi ISO 27001: 2013

Journal of Information System Research (JOSH)
Volume 4, No. 2, Januari 2023, pp 632−640
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i2.2552

(ISMS) di Bagian Komunikasi Satelit Monitoring PT. Bank BRI, TBK," Ikra-Ith Inform. …, vol. 6, no. 2, pp. 21–28, 2022, [Online]. Available: https://journals.upi-yai.ac.id/index.php/ikraith-informatika/article/download/1570/1285.

[19] F. Ainun Nafisah, W. Hayuhardhikai Nugrahai Putra, and H. Admajai Dwi, "Evaluasi Keamanan Informasi Data Center Berdasarkan Standar ISO 27001:2013 (Studi Kasus PT. Pupuk Kalimantan Timur)," vol. 4, no. 6, pp. 1858–1865, 2020, [Online]. Available: http://j-ptiik.ub.ac.id.

[20] D. Rahmat, "Perancangan Sistem Manajemen Keamanan Informasi Menggunakan Standar Sni Iso / Iec 27001 : 2013," J. Inform. – Comput. Vol. 06 Nomor 02, Desember 2019 37-41 ISSN 2656 – 3861, vol. 06, pp. 37–41, 2019.