Analisis Maturity Level Dan PDCA Dalam Penerapan Proses Audit SMKI (Information Security Management System) Menggunakan ISO 27001:2013 Pada PT Indonesia Game

Eri Riana[1,*], Meiva Eka Sri Sulistyawati[2], Octa Pratama Putra [3]

[1,2,3] Program Studi Sistem Informasi; Universitas Bina Sarana Informatika; Jln jatiwaringin Raya No.18, Kota Bekasi Jawa Barat, telp/fax (021) 8462039 e-mail: eri.eea@bsi.ac.id, meiva.mes@bsi.ac.id, octa.opp@bsi.ac.id

* Korespondensi: e-mail: eri.eea@bsi.ac.id

Diterima: 25 November 2022 ; Review: 01 Desember 2022; Disetujui: 06 Desember 2022

Cara sitasi: Riana E, Sulistyawati MES, Putra OP. 2022. Analisis Maturity Level Dan PDCA Dalam Penerapan Proses Audit SMKI (Information Security Management System) Menggunakan ISO 27001:2013 Pada PT Indonesia Game. Informatics for Educators and Professionals. Vol.7 (1): 39 - 50.

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. Dari hasil proses audit dan riset diperoleh di dalam dokumen Klausul 8 dan dokumen Annex 5 mempunyai nilai persentase yang rendah dibandingkan dokumen Klausul dan Annex lainnya, karena dokumentasi yang berkaitan dengan ketidaklengkapan dan ketidaksesuaian dokumen mengenai control A.5.1.1 tentang kebijakan untuk keamanan informasi, serta pada Klausul 8 belum terpenuhi klausul sub klausul 8.1 tentang perencanaan dan pengendalian operasional. Dilihat total penerapan ISO 27001:2013 sudah berjalan baik dengan memiliki hasil tingkat kematangan (maturity level) level 5-Optimised sebesar 93,52%. Dengan hasil seluruh dokumen klausul dan dokumen annex terpenuhi dari standar ISO 27001:2013, diharapkan hasil ini perusahaan bisa kembali melakukan pengembangan dan peningkatan dalam melakukan prosesnya agar mempermudah dari tim audit didalam proses audit internal maupun proses audit eksternal dan bisa terpenuhi keseluruhan sesuai yang terdapat didalam 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. From the results of the audit and research process obtained in the Clause 8 document and Annex 5 document, it has a low percentage value compared to other Clause and Annex documents, because the documentation related to incomplete and non-conforming documents regarding control A.5.1.1 regarding policies for information security, and in Clause 8 the clause sub-clause 8.1 concerning operational planning and control has not been fulfilled. It can be seen that the total implementation of ISO 27001:2013 has been going well with a maturity level of 5-Optimised of 93.52%. With the results of all clause documents and annex documents being fulfilled according to the ISO 27001: 2013 standard, it is hoped that these results will allow the company to continue to develop and improve the process to make it easier for the audit team in the internal audit process and the external audit process and can be fulfilled in full according to what is contained in ISO 27001:2013.

***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 SMKI [4] merupakan pengujian terhadap sisstem keamanan informasi yang ada di dalam suatu organisasi untuk melihat dimana sistem keamanan informasi yang sudah ada sesuai dengan visi, misi dan tujuan organisasi, menguji performa dan untuk mendeteksi resiko dan efek potensial yang mungkin ditimbulkan. Sistem Manajemen Keamanan Informasi adalah suatu proses tindakan preventif dalam hal proses menyalahgunakan sistem informasi dari orang-orang yang menyalahgunakan itu.

ISO 27001:2013 merupakan kerangka didalam menspesifikasikan kebutuhan untuk pembangunan, penerapan, pengawasan dan peningkatan secara kontinue dalam pengaturan individu, pengaturan tersebut dalam sebuah perusahaan hal itu bersifat independent dimana manajemen resiko menjadi prasyarat, serta dirancang dalam penjaminan supaya hal-hal pengaturan system keamanan yang dipergunakan bisa mencegah suatu informasi aset dari beberapa risiko serta memberikan kepercayaan sistem keamanan informasi untuk stakeholder. Bentuk dari ISO 27001:2013 [5] dibagi dalam dua besar yaitu :

1. Dokumen Klausul merupakan syarat untuk perusahaan dalam menerapkan Sistem Manajemen Keamanan Informasi ISO 27001:2013.
2. Dokumen Annex adalah suatu dokumen yang disediakan serta dijadikan acuan didalam menentukan pengawasan keamanan yang perlu diterapkan di dalam SMKI.

Didalam pelaksanaan pengelolaan TIK, hal keamanan adalah sangat penting untuk dilihat dalam hal menghindari resiko [6] didalam penerapan TI, maka PT Indonesia Game menerapkan proses audit didalam terhadap SMKI mempergunakan ISO 27001:2013. Tujuan riset jurnal yang diperoleh yaitu untuk melihat dalam hal tingkat keamanan informasi yang berjalan dalam periode setahun serta memberikan saran-saran untuk PT Indonesia Game supaya dilakukan tindakan-tindakan selanjutnya.

Riset yang dilakukan oleh Bakri dan Irmayana [7], Risetnya berfokus dalam penilaian serta pemetaan permasalahan system keamanan terhadap informasi di SIMHP. penelitian menghasilkan katalog temuan SMKI yang dibuat berdasarkan ISO 27001:2013. Pemetaan diperoleh dengan mengidentifikasikan artifak keamanan informasi, melakukan proses wawancara dan kuisioner kepada Kepala Sub Bagian Prolap dan Administrator. Bentuk pemodelan Sistem Manajemen Keamanan Informasi diproses melalui identifikasi kendali keamanan informasi. Selanjutnya proses penerapan audit dilakukan dengan proses pembuatan pertanyaan, mengidentifikasikan informasi asset, penentuan proses kendali, dan pernyataan berdasarkan dari temuan SMKI. Riset yang dilakukan oleh Sidik, Iriani, dan Yulianto [8]. dimana (ISO) 27001: 2005 dipilih karena framework bisa di sesuaikan dengan instrumen tempat riset tergantung kebutuhan perusahaan serta berfokus ke SMKI. Hasilnya riset JPA = PA1:PA10, NA=JPA/10 mendapatkan total rata-rata 65%, level positif, tapi belum bisa sesuai yang diinginkan oleh perguruan tinggi dimana menginginkan melakukan proses evaluasi yang simultan dan rekomendasi untuk peningkatan control keamanan.

Riset yang dilakukan oleh Heri Wahyudi, Asep Zulianto dan Asep Maulana [9] berdasarkan hasil risetnya di SIMAK bahwa proses audit merupakan proses untuk mengukur kinerja. Agar proses audit SMKI bisa berjalan baik dibutuhkan suatu standar tetapi tidak ada acuan baku

yang dipilih oleh perguruan tinggi dalam melaksanakan audit SMKI sehingga bisa menggunakan standar yang sesuai dengan kebutuhannya.Peneliti merangkum kesimpulan dalam audit SIMAK dimana audit merupakan tahapan kegiatan terdokumentasi dan sistematis untuk memperoleh bukti audit serta melakukan evaluasi objektif dimana untuk menilai kriteria proses audit dapat terpenuhi nantinya. Metode yang dipergunakan yaitu metode kualitatif. Data Primer diperoleh dari wawancara serta tatap muka berserta proses pengamatan langsung. Dimana proses wawancara mengambil informasi kegiatan akademik. Dari hasil penelitiannya mendapatkan identifikasi bahwa dokumen klausul yang dipergunakan merupakan, Kebijakan Keamanan (Security Policy) dokumen annex 5, Manajemen Aset (Asset Management) dokumen annex 7, Kontrol Akses (Access Control) dokumen annex 9 dan Kepatuhan (Compliance) dokumen annex 15.

Sedangkan Penelitian yang dilakukan oleh Siti Alvi Sholikhatin, Arief Setyanto, Emha Taufiq Luthfi [10] bertujuan dalam hal memperoleh posisi keamanan informasi yang sedang berjalan di Universitas Muhammadiyah Purwokerto dan serta membantu penyusunan kebijakan keamanan serta saran untuk peningkatan keamanan informasi sesuai dengan standar. Lain halnya riset oleh Pangky Februari dan Fitria [11] dimana risetnya mengukur standar ISO 27001 di SMKN Pugung. Hasil penelitiannya memperoleh analisis penyebaran kuesioner menghasilkan dengan rata-rata 3,32 di keseluruhan dokumen klausul ISO 27001 kesimpulannya sudah memiliki standar tertulis dan baku.

Riset lain dilakukan oleh Fitroh, Muhamad Rizaldi Seputra, Ginanjar Ramadhan, Tania Nur Hafizah Hersyaf, dan Ari Nur Rokhman [12] Adapun Tujuan dari risetnya mengetahui penerapan ISO 27001 menggunakan sistematika review. sistematika review yang dalam risetnya dimasukan ke dalam empat tahapan yaitu : review identifikasi, penyaringan artikel awal filter artikel lanjutan dan dilanjutkan evaluasi artikel. Hasilnya ditemukan pada masing-masing artikel bernilai 20% Dari hasil riset penerapan ISO 27001 bisa melakukan identifikasi peluang perbaikan dan untuk mengkoordinasikan upaya menujunya kinerja SMKI yang berkelanjutan

Riset oleh Sitta Rif'atul Musyarofah dan Rahadian Bisma [13], dalam risetnya, pembuatan *SOP* didasarkan kebutuhan di Dinas Komunikasi dan Informatika Pemerintah kota Madiun. Pembuatan SOP mengacu ke standar ISO/IEC 27001:2013 dan ISO/IEC 37002:2013 sebagai panduan kontrol keamanan. Dalam pembuatan SOP ini diharapkan mengurangi ancaman keamanan informasi baik dari luar maupun dari dalam perusahaan. Metode yang dipergunakan dengan analisis kesenjangan melalui proses pembandingan kondisi keamanan di Dinas Komunikasi dan Informatika Pemerintah kota Madiun pada saat itu dengan kondisi persyaratan ISO/IEC 27001:2013. Penelitiannya mendapatkan 1 instruksi kerja dan 19 SOP, serta 29 formulir untuk melengkapi prosedur.

Perbedaan riset yang sudah dilakukan dengan yang dilakukan pada saat ini berfokus melakukan audit Sistem Manajemen Keamanan Informasi di PT Indonesia Game dengan standar ISO 27001:2013. Dengan itu akan diperoleh apakah semua dokumen annex dan dokumen klausul yang ada didalam ISO 27001:2013 sudah di terapkan dengan baik ataukah belum di terapkan dengan baik dalam periode satu tahun. Lalu selanjutnya memberikan rekomendasi untuk dokumen annex dan dokumen klausul yang belum diterapkan dengan prosedur didalam PT Indonesia Game. kontribusi dalam riset ini yaitu proses Audit Sistem Manajemen Keamanan Informasi di perusahaan tersebut dengan standar ISO 27001:2013 [14]. Dengan dilakukan riset ini bisa memberi kontribusi positif dalam hal rekomendasi berdasar standar ISO 27001:2013.

2. Metode Penelitian

Berikut ini dijabarkan metode penelitian, bahan pustaka ISO 27001:2013 serta tahapan proses penelitian yang dilakukan.

2.1 ISO 27001:2013

ISO 27001:2013 merupakan suatu standar diterbitkan oleh lembaga International Organization for Standardization (ISO) dan International Electrotechnical Commision (IEC). Sebuah standar Internasional dalam penerapan SMKI atau *Security Management Systems* (ISMS), menjadi salah satu best praktis didalam penerapan keamanan informasi.

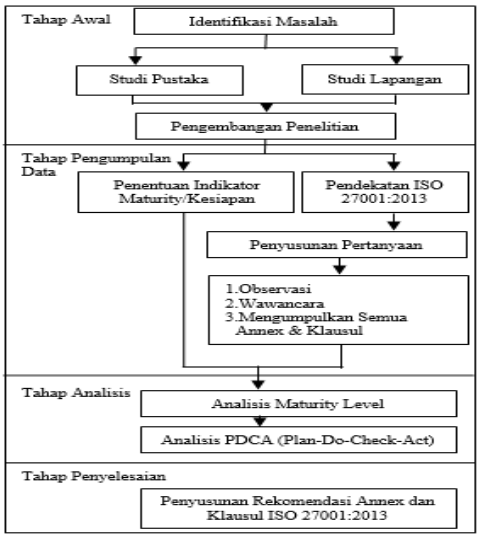
2.2 Keamanan Informasi

Keamanan Informasi merupakan suatu proses keamanan dari keseluruhan ancaman yang bisa saja terjadi dalam upaya untuk memastikan dan menjamin kelangsungan terhadap bisnis organisasi, meminimalkan resiko serta memaksimalkannya. Keamanan sistem informasi adalah suatu bentuk proses perlindungan dan pencegahan gangguan penyalahgunaan yang dilakukan orang yang tidak bertanggung jawab terhadap berjalannya suatu system informasi [15]

2.3 Audit Sistem Informasi

Audit sistem informasi adalah suatu pengujian sistem informasi yang ada dalam suatu perusahaan untuk memastikan apakah sistem informasi yang dimiliki sudah sesuai visi, misi, dan tujuan organisasi serta menguji performance sistem informasi dan mendeteksi risiko efek potensial yang bisa ditimbulkan [16].

Metode penelitian didalam penulisan ini menggunakan metode riset gabungan antara riset kuantitatif dan riset kualitatif, dimana metode riset ini dilakukan dengan cara menggabungkan diantara dua metode riset sekaligus yaitu metode riset kuantitatif dan metode riset kualitatif sehingga didapatkan hasil yang lebih tepat, real, dan komprehensif. Didalam riset jurnal ini, peneliti merancang sebuah kerangka metodologi yang dipergunakan sebagai dasar dari tahapan penelitian sebagaimana yang digambarkan pada gambar 1 berikut ini.



Sumber: Hasil Penelitian (2022)

Gambar 1. Tahapan Penelitian

Berikut merupakan penjelasan dari gambar 1 diatas.

1. Tahap Awal – Identifikasi Masalah

   Identifikasi masalah merupakan tahapan awal mula sebuah riset dilakukan dengan cara mengidentifikasikan masalah. Identifikasi masalah dilakukan untuk mengetahui permasalahan yang akan dianalisa melalui metode yang akan digunakan. Sehingga hasil keseluruhan yang diperoleh sesuai dengan tujuan riset.

   a. Studi Pustaka

      Studi pustaka dari riset ini bermanfaat untuk mengetahui hal-hal yang berkaitan dengan pengetahuan keilmuan terhadap objek yang diteliti. Studi Pustaka didapatkan melalui jurnal internasional dan jurnal nasional serta penelitian-penelitian yang berkaitan terdahulu

   b. Studi Lapangan

Vol. 7, No. 1, Desember 2022, 39 - 50

Studi lapangan dilakukan dengan melihat kondisi di organisasi yang diteliti sekaligus mengumpulkan data-data yang akan diteliti.

c. Pengembangan Penelitian
Pengembangan penelitian dilakukan untuk membandingkan hasil-hasil terdahulu dan hasil-hasil pada saat ini yang diharapkan dari hasil pengembangan tersebut bisa memberikan peningkatan terhadap objek yang diteliti.

2. Tahap Pengumpulan Data – Penentuan Indikator Maturity
Penentuan Indikator maturity digunakan oleh organisasi untuk melakukan evaluasi terhadap sistem manajemen keamanan informasi. Dalam penentuan indikator maturity ini terdapat 5 buah level (level 0 – level 5).

a. Pendekatan ISO 27001-2013
Pendekatan ISO 27001:2013 dipergunakan sebagai pedoman rujukan proses check list saat assessment dalam mengukur tingkat keamanan informasi di suatu organisasi
b. Penyusunan Pertanyaan
Penyusunan pertanyaan (kuisioner) merupakan bagian dari tahap pengumpulan data dengan melakukan pemberian kuisioner. Pemberian kuisioner ini untuk memperoleh mengenai analisis sistem manajemen keamanan informasi.
c. Observasi
Observasi dilakukan untuk memperoleh informasi dan data yang berkaitan dengan objek riset. Dalam riset ini dilakukan dengan cara observasi langsung mengenai keamanan informasi di PT Indonesia Game.
d. Wawancara
Proses wawancara diperoleh dengan tanya jawab secara langsung mengenai hal yang terkait dengan keamanan informasi pada PT Indonesia Game. Tanya jawab dilakukan untuk bisa melihat mengenai keadaaan sistem manajemen keamanan informasi pada PT Indonesia Game dan segala bentuk permasalahannya. Didalam riset ini tanya jawab diperoleh dari tim sistem manajemen keamanan informasi (SMKI) PT Indonesia Game.
e. Pengumpulan Klausul dan Annex
Pengumpulan klausul dan annex merupakan tahapan dari pengumpulan data untuk dijadikan sebagai bahan pengukuran terhadap kelayakan penerapan ISO 27001:2013

3. Tahap Analisis
a. Analisis Maturity Level
Analisis maturity level merupakan suatu tahapan analisis yang berguna bagi organisasi untuk melakukan evaluasi terhadap keamanan informasi. Terdapat adanya 5 buah level didalamnya yaitu level 0 (Non Existent) – level 5 (Optimised).
b. Analisis PDCA
Analisis PDCA [17] merupakan suatu tahapan analisis yang digunakan bagi organisasi sebagai rujukan pedoman yang berkaitan dengan ISO 27001-2013.

4. Tahap Penyelesaian
Tahap ini dilakukan dengan membuat laporan penyusunan rekomendasi terhadap dokumen klausul dan annex yang nantinya dijadikan sebagai bahan pengembangan dan peningkatan bagi manajemen dimasa selanjutnya.

Adapun pengukuran skala maturity level yang dipergunakan akan dijabarkan dalam Tabel 1 berikut ini.

Tabel 1. Skala Maturity level

Level	Skala Index Maturity	Deskripsi
0 - Non Existent	0% - 18%	Tidak didapatkan persoalan yang perlu dibenahi. Organisasi menganggap tidak diperlukan proses keamanan informasi dalam pengawasan internal.
1 - Initial/ Ad Hoc	19% - 36%	Sudah terdapat adanya bukti temuan bahwa organisasi melihat terdapatnya masalah yang memang harus dibenahi. Organisasi sudah memiliki suatu inisiatif dalam melakukan keamanan informasi dimana

Level	Skala Index Maturity	Deskripsi
		diperlukan pengawasan internal
2 - Repeatable but Intuitive	37% - 54%	Sudah terdapat adanya suatu pengelolaan, perencanaan, , dan penerapan sistem yang lebih berfokus. Organisasi mempunyai kebiasaan terpola dalam melakukan perencanaan keamanan informasi yang dilakukan secara berulang-ulang namun tidak melibatkan dokumen yang bersifat formal/tidak adanya dokumentasi
3 - Defined	56% - 72%	Sudah mempunyai suatu proses keamanan informasi yang terdokumentasi dengan baik. Organisasi menyadari pentingnya suatu proses keamanan informas sehingga ada suatu aturan dimana menunjukkan untuk organisasi secara kontinue melakukan proses keamanan
4 - Managed and Measurable	73% - 90%	Sudah adanya suatu pengaturan internal yang efektif dan terarah. Proses keamanan informasi secara formal dilakukan dan adanya penanganan manajemen resiko
5- Optimised	91% - 100%	Sudah menerapkan best practice dalam sebuah pengaturan dan analisis suatu resiko yang berkesinambungan dan efektif

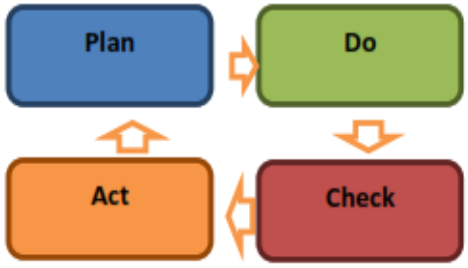
Sumber: Hasil Penelitian (2022)

Dalam pengukuran tingkat kematangan dokumen Annex dan dokumen Klausul menggunakan rumus index maturity seperti berikut ini (1).

$$\text{Index } Maturity = \frac{\text{Jumlah pertanyaan yang dijawab}}{\text{Jumlah pertanyaan klausul dan annex}} \times 100 \,(1)$$

Didalam rumus index maturity (1) dijelaskan cara untuk memperoleh tingkat kematangan dokumen Klausal dan dokumen Annex, dengan menghitung jumlah kuisioner/pertanyaan yang dijawab dikali bobot dari setiap jawaban yang sudah ditentukan lalu dibagi total kuisioner/pertanyaan. Skala likert diajukan untuk pemilihan jawaban dimana ada 6 jawaban dalam tingkat kematangan.

Selanjutnya dilakukan dengan tahap analisis mengenai PDCA (*Plan-Do-CheckAct*), Adapun gambaran tahapan PDCA dijelaskan dalam gambar 2 dan table 2 berikut ini :



Sumber: Hasil Penelitian (2022)

Gambar 2. Diagram Siklus PDCA

Berikut merupakan penjelasan dari gambar 1 diatas, melalui table 2.

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

Tahapan Siklus	Keterangan
Plan	Suatu tahapan yang digunakan dalam kebijakan perencanaan SMKI dan perancangan SMKI. Misalnya melakukan komitmen, melakukan control, melakukan prosedur, melakukan instruksi kerja dan kebijakan-kebijakan lainnya sehingga akan terbentuk SMKI yang diinginkan oleh organisasi.
Do	Suatu tahapan penerapan dari komitmen, control, prosedur, instruksi kerja dan kebijakan-kebijakan lainnya yang sudah dicanangkan dalam tahap Plan
Check	Suatu tahapan yang dilakukan untuk pengawasan sistem manajemen keamanan informasi, pengukuran kinerja SMKI apakah sudah sesuai atau belum sesuai. Bila belum sesuai dilakukan proses audit dan evaluasi terhadap sistem manajemen keamanan informasi.
Act	Suatu tahapan dari suatu pengembangan dengan melakukan suatu langkah-langkah pencegahan dan melakukan langkah-langkah

	koreksi, yang kesemuanya itu merupakan tahapan perbaikan dan pengembangan untuk peningkatan sistem manajemen keamanan informasi yang berkesinambungan.

Sumber: Hasil Penelitian (2022)

3. Hasil dan Pembahasan

3.1 Analisis Maturity Level

Untuk analisis tingkat kematangan terhadap penerapan SMKI, PT Indonesia Game melakukan beberapa analisis seperti melakukan analisis terhadap suatu dokumen, melakukan pengamatan secara langsung, melakukan tatap muka tanya jawab (wawancara) dengan beberapa bagian terkait dicocokan dengan checklist data dan disesuaikan dengan pedoman pada ISO 27001:2013. Berikut hasil dari analisis maturity levelnya pada Tabel 3 [18].

Tabel 3. Nilai Pengukuran Maturity Level

Analisis Dokumen Annex dan Analisis Dokumen Klausul	Skala Tingkat Kematangan %	Level Tingkat Kematangan
Analisis Klausul 4 Konteks Organisasi	100%	5 - Optimised
Analisis Klausul 5 Kepemimpinan	100%	5 - Optimised
Analisis Klausul 6 Perencanaan	91,74%	5 - Optimised
Analisis Klausul 7 Dukungan	100%	5 - Optimised
Analisis Klausul 8 Operasi	73,15%	4 - Managed and Measurable
Analisis Klausul 9 Evaluasi Kinerja	100%	5 - Optimised
Analisis Klausul 10 Perbaikan	100%	5 - Optimised
Analisis (A5) Annex 5 Kebijakan Keamanan Informasi	71,12%	3 - Defined Process
Analisis (A6) Annex 6 Organisasi keamanan informasi	100%	5 - Optimised
Analisis (A7) Annex 7 Keamanan sumber daya manusia	74,23%	4 - Managed and Measurable
Analisis (A8) Annex 8 Manajemen aset	93,60%	5 - Optimised
Analisis (A9) Annex 9 Kendali akses	100%	5 - Optimised
Analisis (A10) Annex 10 Kriptografi	100%	5 - Optimised
Analisis (A11) Annex 11 Keamanan fisik dan lingkungan	100%	5 - Optimised
Analisis (A12) Annex 12 Keamanan operasi	100%	5 - Optimised
Analisis (A13) Annex 13 Keamanan komunikasi	87,61%	4 - Managed and Measurable
Analisis (A14) Annex 14 Akuisisi , pengembangan dan perawatan sistem	86,60%	4 - Managed and Measurable
Analisis (A15) Annex 15 Hubungan Pemasok	100%	5 - Optimised
Analisis (A16) Annex 16 Manajemen insiden keamanan informasi	85,89%	4 - Managed and Measurable
Analisis (A17) Annex 17 Aspek keamanan informasi dari manajemen keberlangsungan bisnis	100%	5 - Optimised
Analisis (A18) Annex 18 Kesesuaian	100%	5 - Optimised
Total Maturity Level	**93,52%**	

Sumber: Hasil Penelitian (2022)

Dari penjabaran dalam Table 3 hasil pengukuran analisis tingkat kematangan pada setiap bagian klausul dan annex dijelaskan sebagai berikut :

1. Analisis Klausul 4 Konteks Organisasi
   Klausul 4 Konteks Organisasi memiliki persentasi nilai hasil 100% masuk kedalam level 5-Optimised hal ini menunjukkan proses dokumentasi audit telah lengkap dan persyaratan

yang terdapat pada Konteks Organisasi telah berjalan dengan baik dan sudah sesuai dengan ISO 27001:2013.

2. Analisis Klausul 5 Kepemimpinan
   Klausul 5 Kepemimpinan memiliki persentasi nilai hasil 100% masuk kedalam level 5-Optimised hal ini menunjukkan bahwa semua kebijakan-kebijakan sudah di dokumentasikan dengan lengkap saat audit dan persyaratan yang terdapat pada Kepemimpinan telah berjalan dengan baik dan sudah sesuai dengan ISO 27001:2013.
3. Analisis Klausul 6 Perencanaan
   Klausul 6 Perencanaan memiliki persentasi nilai hasil 91,74% masuk kedalam level 5-Optimised hal ini menunjukkan proses dokumentasi audit sudah cukup lengkap dan sudah sesuai dengan ISO 27001:2013, namun ada beberapa pedoman yang perlu di revisi.
4. Analisis Klausul 7 Dukungan
   Klausul 7 Dukungan memiliki persentasi nilai hasil 100% masuk kedalam level 5-Optimised hal ini menunjukkan proses dokumentasi audit telah lengkap dan persyaratan yang terdapat pada Dukungan telah berjalan dengan baik dan sudah sesuai dengan ISO 27001:2013.
5. Analisis Klausul 8 Operasi
   Klausul 8 Operasi memiliki persentasi nilai hasil 73,15% masuk kedalam level 4-Managed and Measurable hal ini menunjukkan terdapat banyaknya syarat yang belum terpenuhi pada sub klausul 8.3 seperti penilaian risiko keamanan dimana belum terdapatnya dokumen planning penilaian resiko keamanan informasi yang akan diterapkan. Klausul yang belum terpenuhi juga terdapat pada klausul sub klausul 8.1 tentang perencanaan dan pengendalian operasional. Sedangkan persyaratan yang sudah terpenuhi terdapat di sub klausul 8.2 mengenai penanganan resiko keamanan informasi.
6. Analisis Klausul 9 Evaluasi Kinerja
   Klausul 9 Evaluasi Kinerja memiliki persentasi nilai hasil 100% masuk kedalam level 5-Optimised hal ini menunjukkan proses dokumentasi audit telah lengkap dan persyaratan yang terdapat pada Evaluasi Kerja telah berjalan dengan baik dan sudah sesuai dengan ISO 27001:2013.
7. Analisis Klausul 10 Perbaikan
   Klausul 10 Perbaikan memiliki persentasi nilai hasil 100% masuk kedalam level 5-Optimised hal ini menunjukkan proses dokumentasi audit telah lengkap dan persyaratan yang terdapat pada Perbaikan telah berjalan dengan baik dan sudah sesuai dengan ISO 27001:2013.
8. Analisis (A5) Annex 5 Kebijakan Keamanan Informasi
   (A5) Annex 5 Kebijakan Keamanan Informasi memiliki persentasi nilai hasil 71,12% masuk kedalam level 3-Defined Process hal ini menunjukkan bahwasannya belum memenuhi persyaratan dalam penerapan keamanan informasi. Hal yang tidak sesuai dan belum terpenuhi mengenai control 5.1.1 berkaitan dengan kebijakan untuk keamanan informasi. Sedangkan persyaratan yang sudah terpenuhi terdapat 5.1 mengenai arahan manajemen untuk keamanan informasi.
9. Analisis (A6) Annex 6 Organisasi keamanan informasi
   (A6) Annex 6 Organisasi keamanan informasi memiliki persentasi nilai hasil 100% masuk kedalam level 5-Optimised hal ini menunjukkan proses dokumentasi audit telah lengkap dan persyaratan yang terdapat pada Organisasi Keamanan Informasi telah berjalan dengan baik dan sudah sesuai dengan ISO 27001:2013.
10. Analisis (A7) Annex 7 Keamanan sumber daya manusia
    (A7) Annex 7 Keamanan sumber daya manusia memiliki persentasi nilai hasil 74,23% masuk kedalam level 4- Managed and Measurable hal ini menunjukkan bahwa syarat pada Annex 7 telah dilakukan cukup baik tetapi belum terpenuhi sepenuhnya diimplementasikan. Ketidaklengkapan terjadi pada control 7.2.2 mengenai kepedulian, Pendidikan dan pelatihan keamanan informasi. Dari hal ini perlu dilakukan pelatihan akan perlunya keamanan informasi.
11. Analisis (A8) Annex 8 Manajemen asset
    (A8) Annex 8 Manajemen asset memiliki persentasi nilai hasil 93,60% masuk kedalam level 5-Optimised hal ini menunjukkan proses dokumentasi audit sudah cukup lengkap dan persyaratan yang terdapat pada Manajemen Asset telah berjalan dengan baik dan sudah

sesuai dengan ISO 27001:2013. Namun ketidaklengkapan terjadi pada 8.1.1 mengenai inventaris asset dimana belum adanya suatu prosedur yang dapat diterima.

12. Analisis (A9) Annex 9 Kendali akses
    (A9) Annex 9 Kendali akses memiliki persentasi nilai hasil 100% masuk kedalam level 5-Optimised hal ini menunjukkan proses dokumentasi audit telah lengkap dan persyaratan yang terdapat pada Kendali Akses telah berjalan dengan baik dan sudah sesuai dengan ISO 27001:2013.
13. Analisis (A10) Annex 10 Kriptografi
    (A10) Annex 10 Kriptografi memiliki persentasi nilai hasil 100% masuk kedalam level 5-Optimised hal ini menunjukkan proses dokumentasi audit telah lengkap dan persyaratan yang terdapat pada Kriptografi telah berjalan dengan baik dan sudah sesuai dengan ISO 27001:2013.
14. Analisis (A11) Annex 11 Keamanan fisik dan lingkungan
    (A11) Annex 11 Keamanan fisik dan lingkungan memiliki persentasi nilai hasil 100% masuk kedalam level 5-Optimised hal ini menunjukkan proses dokumentasi audit telah lengkap dan persyaratan yang terdapat pada Keamanan Fisik dan Lingkungan telah berjalan dengan baik dan sudah sesuai dengan ISO 27001:2013.
15. Analisis (A12) Annex 12 Keamanan operasi
    (A12) Annex 12 Keamanan operasi memiliki persentasi nilai hasil 100% masuk kedalam level 5-Optimised hal ini menunjukkan proses dokumentasi audit telah lengkap dan persyaratan yang terdapat pada Keamanan Operasi telah berjalan dengan baik dan sudah sesuai dengan ISO 27001:2013.
16. Analisis (A13) Annex 13 Keamanan komunikasi
    (A13) Annex 13 Keamanan komunikasi memiliki persentasi nilai hasil 87,61% masuk kedalam level 4- Managed and Measurable hal ini menunjukkan bahwa adanya aggrement mengenai kerahasiaan system jaringan organisasi yang berkaitan juga dengan keamanan jaringan. Ketidaklengkapan terjadi pada control 13.2.2 mengenai perjanjian perpindahan informasi dimana belum adanya dokumentasi prosedur hal tersebut.
17. Analisis (A14) Annex 14 Akuisisi , pengembangan dan perawatan system
    (A14) Annex 14 Akuisisi, pengembangan dan perawatan system memiliki persentasi nilai hasil 86,60% masuk kedalam level 4- Managed and Measurable hal ini menunjukkan didalam proses penentuan system baru yang sudah dilihat mengenai system keamanan informasi. Didalam proses pengembangan dan perawatan system diatur dalam prosedur dan kebijakan pengembangan.Tapi hal ini tetap perlu di evaluasi kembali dalam proses pengembangannya. Ketidaklengkapan terjadi pada control 14.2.1 mengenai kebijakan pengembangan yang aman dimana belum terdapatnya prosedur tersebut.
18. Analisis (A15) Annex 15 Hubungan Pemasok
    (A15) Annex 15 Hubungan Pemasok memiliki persentasi nilai hasil 100% masuk kedalam level 5-Optimised hal ini menunjukkan proses dokumentasi audit telah lengkap dan persyaratan yang terdapat pada Hubungan Pemasok telah berjalan dengan baik dan sudah sesuai dengan ISO 27001:2013.
19. Analisis (A16) Annex 16 Manajemen insiden keamanan informasi
    (A16) Annex 16 Manajemen insiden keamanan informasi memiliki persentasi nilai hasil 85,89% masuk kedalam level 4-Managed and Measurable hal ini menunjukkan ada beberapa syarat yang belum terpenuhi yang terjadi pada control 15.1.2 yang berkaitan dengan akses pemasok.
20. Analisis (A17) Annex 17 Aspek keamanan informasi dari manajemen keberlangsungan bisnis
    (A17) Annex 17 Aspek keamanan informasi dari manajemen keberlangsungan bisnis memiliki persentasi nilai hasil 100% masuk kedalam level 5-Optimised hal ini menunjukkan proses dokumentasi audit telah lengkap dan persyaratan yang terdapat pada Aspek keamanan informasi dari manajemen keberlangsungan bisnis telah berjalan dengan baik dan sudah sesuai dengan ISO 27001:2013.
21. Analisis (A18) Annex 18 Kesesuaian
    (A18) Annex 18 Kesesuaian memiliki persentasi nilai hasil 100% masuk kedalam level 5-Optimised hal ini menunjukkan proses dokumentasi audit telah lengkap dan persyaratan yang terdapat pada Kesesuaian telah berjalan dengan baik dan sudah sesuai dengan ISO 27001:2013.

Dapat dilihat bahwa pada Klausul 8 dan Annex 5 mempunyai nilai persentase yang rendah sebesar 71,12% (Annex 5) dan 73,15% (Klausul 8). Disebabkan oleh ketidaklengkapan dan ketidaksesuaian dokumen mengenai control A.5.1.1 berkaitan dengan kebijakan untuk keamanan informasi, serta pada Klausul 8 belum terpenuhi klausul sub klausul 8.1 tentang perencanaan dan pengendalian operasional. Dari ketidaklengkapan dan ketidaksesuaian tersebut menyebabkan klausul dan annex mempunyai nilai yang rendah tingkat kematangannya. Didapatkan nilai persentase rata-rata hasil tingkat kematangan ISO 27001:2013 pada PT Indonesia Game 93,52% skala tingkat kematangan 5-Optimised. Dapat disimpulkan bahwa ISO 27001:2013 telah terdokumentasi dengan baik hanya saja perlu adanya peningkatan dan pengembangan kembali mengenai prosedur dan kebijakan-kebijakan yang terdapat pada klausul dan annexnya.

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

Untuk melakukan analisis PDCA dilakukan dengan melalui pengamatan dan proses penilaian menggunakan check list yang disesuaikan dengan standar ISO 27001:2013 serta disesuaikan dengan analisis PDCA [19], Didalam siklus *Plan* Menyusun kebijakan system manajeman keamanan informasi, proses yang analisis antara lain:

1. Menyusun kebijakan Sistem Manajemen Keamanan Informasi, objektif, proses dan prosedur.
2. Melakukan pengelolaan risk.
3. Mengevaluasi dan menganalisis risk.
4. Melakukan pengelolaan keamanan informasi.

Kemudian didalam siklus *Do* kegiatan yang dianalisis:

1. Pengelolaan operasi dan sumberdaya Sistem Manajemen Keamanan Informasi.
2. Menerapkan kegiatan pelatihan dan kesadaran akan mengenai Sistem Manajemen Keamanan Informasi.
3. Menerapkan kebijakan control dan kebijakan prosedur yang dapat melakukan deteksi terhadap keamanan informasi serta dapat melakukan respon.

Proses siklus ketiga yaitu *Check* meliputi:

1. Melakukan monitor dan mereview keseluruhan kontrol-kontrol dan prosedur-prosedur yang sudah berjalan.
2. Melakukan proses pengecekan secara berkelanjutan mengenai kelayakan Sistem Manajemen Keamanan Informasi.
3. Mengadakan audit internal Sistem Manajemen Keamanan Informasi .
4. Melakukan update planning Sistem Manajemen Keamanan Informasi.
5. Mendokumentasikan semua klausul dan annex untuk mendukung kelayakan dari kinerja sistem manajemen keamanan informasi.

Proses siklus keempat didalam PDCA yaitu *Act* yaitu :

1. Menerapkan proses pengembangan Sistem Manajemen Keamanan Informasi.
2. Menjalankan proses kegiatan pencegahan dan koreksi.
3. Memberikan informasi kepada semua bagian yang terkait apabila terdapat adanya suatu kegiatan dan peningkatan atau pengembangan.
4. Memastikan bahwa semua peningkatan telah berjalan sesuai dengan objek yang teridentifikasi

4. Kesimpulan

Dari hasil proses audit dan riset diperoleh di dalam dokumen Klausul 8 dan Annex 5 mempunyai nilai persentase yang rendah sebesar 71,12% (Annex 5) dan 73,15% (Klausul 8). Disebabkan oleh ketidaklengkapan dan ketidaksesuaian dokumen mengenai control A.5.1.1 berkaitan dengan kebijakan untuk keamanan informasi, serta pada Klausul 8 belum terpenuhi klausul sub klausul 8.1 tentang perencanaan dan pengendalian operasional. Dari ketidaklengkapan dan ketidaksesuaian tersebut menyebabkan klausul dan annex mempunyai nilai yang rendah tingkat kematangannya. Dilihat total penerapan ISO 27001:2013 sudah berjalan baik dengan memiliki hasil tingkat kematangan level 5 sebesar 93,52%. Dengan hasil

seluruh dokumen klausul dan dokumen annex terpenuhi dari standar ISO 27001:2013, diharapkan hasil ini perusahaan bisa melakukan pengembangan ataupun peningkatan dalam melakukan proses-prosesnya untuk mempermudah dari tim audit dalam audit internal maupun audit eksternal dan bisa terpenuhinya keseluruhan sesuai yang terdapat didalam ISO 27001:2013.

Ucapan Terima Kasih

Terima kasih disampaikan kepada pihak-pihak yang telah mendukung terlaksananya penelitian jurnal ini.

Referensi

[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] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.
[14] I. Yustiana, “Perancangan Tata Kelola Keamanan Informasi Menggunakan Kerangka Kerja Cobit 5,” pp. 1–9, 2017.
[15] Suharjanti, “Prosiding Seminar Nasional Aplikasi Sains & Teknologi (SNAST) 2014 Yogyakarta, 15 November 2014 ISSN: 1979-911X,” *Snast*, no. November, pp. 211–216, 2014.
[16] 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.
[17] S. T. Yuwono, N. Pratama, and V. Afifah, “Re-Assessment Konsistensi Dokumen Kontrol Sertifikasi ISO 27001: 2013 (ISMS) di Bagian Komunikasi Satelit Monitoring PT. Bank BRI, TBK,” *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.
[18] 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.
[19] 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.