AUDIT SISTEM MANAJEMEN KEAMANAN INFORMASI PUSAT TEKNOLOGI INFORMASI DAN KOMUNIKASI PENERBANGAN DAN ANTARIKSA (PUSTIKPAN) MENGGUNAKAN SNI ISO/IEC 27001:2013

Yudhistira Candra Pradipta[1)], Yani Rahardja[2)], dan **Melkior N.N. Sitokdana[3)]**

[1,2,3]Program Studi Sistem Informasi, Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
[1,2,3]Jalan Diponegoro No. 52-60, Salatiga 50711, Indonesia
E-mail: candra_yudhis@yahoo.co.id[1)], yani.rahardja@uksw.edu[2)], melkior.sitokdana@uksw.edu[3)]

ABSTRAK

Penerapan tata kelola Teknologi Informasi dan Komunikasi (TIK) saat ini sudah menjadi kebutuhan dan tuntutan di setiap instansi penyelenggara pelayanan publik mengingat peran TIK yang semakin penting bagi upaya peningkatan kualitas layanan sebagai salah satu realisasi dari tata kelola pemerintahan yang baik (*Good Corporate Governance*). Untuk maksud tersebut maka perlu dilakukan penelitian untuk mengaudit Sistem Manajemen Keamanan Informasi di Pusat Teknologi Informasi dan Komunikasi Penerbangan dan Antariksa (PUSTIKPAN) menggunakan ISO/IEC 27001:2013. Berdasarkan hasil penelitian tersebut ditemukan bahwa bahwa Annex 7 memiliki tingakatan paling rendah diantara Annex lainnyadikarenakan pada dokumen intruksi kerja terkait labeling belum terdaftar dalam dokumen induk sehingga perlu disesuaikan kembali dokumen induknya. Selain itu, masih ada dari klausul dan annex lainnya masih terdapat beberapa dokumen dan formulir yang kurang sesuai antara judul dengan yang tercantum pada kebijakan/prosedur yang ada sehingga kurang adanya sinkronisasi. Kemudian secara keseluruhan penggunaan ISO/IEC 27001:2013 telah terlaksana dengan baik karena memiliki rata-rata nilai *maturity level* 97,25% dengan level 5 *Optimised.* Hampir dari seluruh klausul dan annex memenuhi standar ISO/IEC 27001:2013 terlaksana sehingga dari hasil penelitian ini diharapkan PUSTIKPAN dapat meningkatkan kembali dalam pengarsipan dokumen agar memudahkan auditor dalam melakukan audit internal ataupun eksternal serta dapat terlaksananya seluruh kegiatan sesuai dengan standar ISO/IEC 27001:2013.

***Kata Kunci** : Audit Sistem Informasi, Tata Kelola, Manajemen Keamanan, Teknologi Informasi, ISO/IEC 27001:2013*

1. PENDAHULUAN

Penerapan tata kelola Teknologi Informasi dan Komunikasi (TIK) saat ini sudah menjadi kebutuhan dan tuntutan di setiap instansi penyelenggara pelayanan publik mengingat peran TIK yang semakin penting bagi

kinerja tata kelola TIK akan terganggu jika informasi sebagai salah satu objek utama tata kelola TIK mengalami masalah keamanan informasi yang menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*).

Lembaga Penerbangan dan Antariksa Nasional (LAPAN) adalah Lembaga Pemerintah Non Kementerian (LPNK) yang mempunyai tugas melaksanakan tugas pemerintahan di bidang penelitian dan pengembangan penerbangan dan antariksa dan pemanfaatannya serta penyelenggaraan keantariksaan sesuai dengan ketentuan peraturan perundang-undangan yang berlaku. LAPAN memiliki unsur pendukung pelaksanaan tugas dan fungsi LAPAN di bidang teknologi informasi dan komunikasi penerbangan dan antariksa yaitu Pusat Teknologi Informasi dan Komunikasi Penerbangan dan Antariksa

standar ini adalah standar ini fleksibel dikembangkan karena sangat tergantung dari kebutuhan organisasi, tujuan organisasi, persyaratan keamanan dan juga SNI ISO/IEC 27001:2013 menyediakan sertifikat upaya peningkatan kualitas layanan sebagai salah satu realisasi dari tata kelola pemerintahan yang baik (*Good Corporate Governance*). Dalam penyelenggaraan tata kelola TIK, faktor keamanan informasi merupakan aspek yang sangat penting diperhatikan mengingat (PUSTIKPAN). PUSTIKPAN memiliki tugas yaitu melaksanakan pengelolaan infrastruktur dan layanan teknologi informasi dan komunikasi, keamanan informasi, sistem informasi, serta tata kelola teknologi informasi dan komunikasi.

Dalam menghindari resiko-resiko dalam penggunaan TI tersebut, maka PUSTIKPAN melakukan audit internal terhadap Sistem Manajemen Keamanan Informasi menggunakan ISO/IEC 27001:2013. Untuk meningkatkan keamanan informasi , Diperlukan audit internal pada Pusat Teknologi Informasi dan Komunikasi Penerbangan dan Antariksa (PUSTIKPAN) untuk memastikan keamanan informasi diterapkan sesuai prosedur. Standar yang digunakan yaitu SNI ISO/IEC 27001:2013. Beberapa hal yang menjadi pertimbangan dalam penggunaan implementasi Sistem Manajemen Keamanan Informasi SMKI yang diakui secara nasional dan internasional yang disebut Information Security Management System ISMS (Direktorat Keamanan Informasi 2011:09).

Tujuan penelitian yang akan dihasilkan pada hasil audit internal menggunakan SNI ISO/IEC 27001:2013 yaitu untuk mengetahui tingkat keamanan informasi yang terjadi selama satu tahun dan memberi rekomendasi untuk LAPAN untuk di lakukan tindakan taktis maupun strategis.Penelitian tentang audit teknologi informasi menggunakan ISO 27001 bukan merupakan penelitian terbaru maka beberapa penelitian terdahulu di jadikan sebagai acuan dalam penelitian ini Antara lain.

Penelitian dengan judul Audit Manajemen Keamanan Teknologi Informasi Menggunakan Standar ISO 27001:2005 Di Perguruan Tinggi XYZ. Standar yang digunakan framework *International Standarization Organization* (ISO) 27001: 2005 dipilih karena framework tersebut dapat di sesuaikan dengan instrumen tempat penelitian tergantung pada kebutuhan organisasi dikembangkan dan difokuskan pada Sistem Manajemen Keamanan Informasi (SMKI). Hasil keseluruhan penelitian JPA = PA1:PA10, NA=JPA/10 menghasilkan nilai akhir rata-rata 65%. Berarti, menunjukan level positif, namun belum sesuai yang diharapkan oleh perguruan tinggi yang mengharuskan melakukan evaluasi yang berkesinambungan dan peningkatan control keamanan yang telah direkomendasikan (Sidik, Iriani and Yulianto, 2018).

Penelitian dengan judul Analisis Sistem Manajemen Keamanan Informasi Menggunakan ISO/IEC 27001:2013 Serta Rekomendasi Model Sistem Menggunakan Data Flow Diagram pada Direktorat Sistem Informasi Perguruan Tinggi. Tujuan dari penelitian ini adalah untuk mengukur tingkat keamanan informasi berdasarkan standar ISO/IEC 27001:2013 dan pemodelan sistem manajemen keamanan informasi. Penelitian ini menggunakan jenis pendekatan kualitatif deskriptif, teknik pengumpulan dan validasi data dengan teknik tringulasi (wawancara, observasi dan dokumentasi). Analisis data dilakukan dengan gap analysis dan untuk mengukur tingkat kematangan penelitian ini mengunakan SSE-CMM (*Systems Security Engineering Capability Maturity Model).* Berdasarkan hasil penelitian, *maturity level* pada klausul kebijakan keamanan informasi mencapai level 1 (*Performed-Informally*), klausul manajemen aset mencapai level 3 (Well-Defined), klausul kontrol akses mencapai level 3 *(Well-Defined),* klausul keamanan fisik dan lingkungan mencapai level 3 *(WellDefined),* klausul keamanan operasional mencapai level 3 *(Well-Defined),* klausul keamanan komunikasi mencapai level 2 (*Planned and Tracked*). Berdasarkan hasil penilaian maturity level ditemukan beberapa kekurangan pada manajemen aset dalam mengimplementasikan kebijakan. Oleh karena itu, pemodelan sistem dengan menggunakan flow map dan CD/DFD difokuskan pada sistem manajemen aset (Yuze, Priyadi and Candiwan, 2016).

Penelitian dengan judul Keamanan Informasi SIMHP BPKP Menggunakan Standar ISO 27001. Penelitian ini berfokus pada penilaian dan pemetaan permasalahan keamanan terhadap aset informasi pada SIMHP. Berdasarkan penelitian dihasilkan katalog temuan-temuan SMKI yang dibuat berdasarkan dari standar Internasional yang diterapkan oleh ISO 27001:2013. Pemataan telah dilakukan dengan cara mengidentifikasi artifak keamanan informasi pada SIMHP, melakukan kuisioner dan wawancara terhadap Kepala Sub Bagian Prolap dan Administrator SIMHP. Pemodelan SMKI telah dilakukan dengan cara mengidentifikasi kendali-kendali keamanan informasi. Kemudian langkah pelaksanaan audit keamanan sistem informasi dilakukan dengan pembuatan pernyataan, identifikasi asset informasi, pembuatan pertanyaan, penentuan kendali berdasarkan temuan-temuan SMKI(Bakri and Irmayana, 2017).

Penelitian dengan judul Audit Internal Keamanan Sistem Informasi Keuangan Stekom Menggunakan Acunetix Tools Dengan Standart SMKI. Berdasarkan hasil temuan audit keamanan sistem informasi yang telah dilakukan dengan menggunakan ISO 27001 dengan monitoring dan tinjauan SMKI dan perhitungan maturity level diketahui dengan melakukan pengamatan secara langsung dan wawancara kepada pihak Koordinator STEKOM diperoleh data bahwa sistem manajemen keamanan informasi (SMKI) maturity level berada pada level 3,35. Hal ini menunjukkan bahwa masih banyak perbaikan yang harus dilakukan pada sistem keamanan(Kusumajaya, Sembiring and Purnomo, 2010).

Penelitian dengan judul Analisa Manajemen Resiko Keamanan Informasi pada Kantor Pelayanan Pajak Pratama XYZ. Data dan informasi yang terdapat pada Lembaga ini tidak hanya perlu penyimpanan secara digital akan tetapi juga memerlukan pengamanan yang serius. Kebocoran akan data yang ada dapat berakibat fatal bagi kepentingan negara. Untuk itu Sistem Manajemen Keamanan Informasi(SMKI) diperlukan dalam pengelolaan keamanannya. Dalam mengimplementasikan ISO 27001 sebelumnya diperlukan manajemen resiko keamanan informasi. Kegiatan manajemen resiko ini diperlukan untuk menentukan Control Objectives yang akan diambil untuk melakukan penanganan resiko yang kemungkinan terjadi. Dalam mengimplementasikan manajemen resiko didapatkan hasil hanya pada aset username dan password level yang resikonya High (6,67%) dari 15 aset yang sudah terdaftar, sehingga diperlukan kontrol keamanan yang berhubungan dengan username dan password untuk meminimalisir atau mengurangi terjadinya resiko(Santosa and Kuswanto, 2016).

Perbedaan penelitian yang sudah dilakukan oleh peneliti terdahulu dengan yang dilakukan ini adalah pada penelitian ini fokus mengaudit manajemen keamanan informasi di PUSTIKPAN menggunakan SNI ISO/IEC 27001:2013. Dengan kajian ini tentu akan mengetahui apakah semua klausul dan annex yang terdapat dalam buku SNI ISO/IEC 27001:2013 sudah di implementasikan dengan baik atau belum dalam satu tahun terakhir. Kemudian selanjutnya diberikan rekomendasi untuk klausul dan annex yang belum

terimplemtasi dengan prosedur yang ada dalam instansi Pusat Teknologi Informasi dan Komunikasi Penerbangan dan Antariksa (PUSTIKPAN). Unsur kebaruan dan kontribusi dalam penelitian ini adalah Audit Sistem Manajemen Keamanan Informasi pada organisasi tersebut menggunakan SNI ISO/IEC 27001:2013 merupakan hal baru yang belum pernah dilakukan oleh peneliti sebelumnya. Oleh karena itu, dengan penelitian ini diharapkan dapat memberikan kontribusi berupa rekomendasi-rekomendasi berdasarkan standar SNI ISO/IEC 27001:2013.

2. RUANG LINGKUP

Ruang lingkup penelitian ini adalah sebagai berikut :

1. Cakupan permasalahan dalam penelitian ini adalah pelaksanaan audit internal di Lembaga Penerbangan dan Antariksa Nasional (LAPAN) selama ini dilakukan selama dua kali dalam satu tahun dan dalam tahun 2018 baru dilakukan hanya satu kali. Oleh karena itu, dibutuhkan audit internal dimana dalam audit internal ini hanya fokus terhadap klausul dan annex pada buku SNI ISO/IEC 27001:2013 sebagai acuan keamanan informasi.
2. Batasan penelitian ini hanyafokus pada sistem manajemen kemanan infomasi (SMKI) pada Pusat Teknologi Informasi dan Komunikasi Penerbangan dan Antariksa (PUSTIKPAN).
3. Rencana hasil yang didapatkan dari penelitian ini adalah membantu instansi dalam audit internal dan mengetahui tingkat kematangan pada sistem manajemen keamanan informasi (SMKI).

3. BAHAN DAN METODE

Berikut disajikan bahan kajian, metode dan tahapan penelitian yang dilakukan :

3.1 Audit Sistem Informasi

Audit sistem informasi adalah cara untuk melakukan pengujian terhadap sistem informasi yang ada di dalam organisasi untuk mengetahui apakah sistem informasi yang dimiliki telah sesuai dengan visi, misi dan tujuan organisasi, menguji performa sistem informasi dan untuk mendeteksi risiko-risiko dan efek potensial yang mungkin timbul (Ramdhany and Asikin, 2018).

Sistem informasi adalah suatu sistem didalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian yang mendukung fungsi organisasi yang bersifat manajerial dalam kegiatan strategi dari suatu organisasi untuk dapat menyediakan kepada pihak luar tertentu dengan laporan-laporan yang diperlukan, dimana sumber daya manusia, komputer dikoordinasikan untuk mengubah masukan (data) menjadi keluaran (informasi), untuk mencapai sasaran perusahaan sesuai dengan visi dan misi perusahaan. Menurut Turban, McLean, dan Wetherbe (1999) sistem informasi mengumpulkan memperoses, menyimpan, menganalisis, dan menyebarkan informasi untuk tujuan yang spesifik(Indrawati and Hernikawati, 2016). Sedangkan Menurut Wilkinson (1992) Sistem informasi adalah kerangka kerja yang mengoordinasikan sumber daya (manusia, komputer) untuk mengubah masukan (*input*) menjadi keluaran (informasi), guna mencapai sasaran-sasaran perusahaan (Kadir, 2014).

3.2 Keamanan Informasi

Keamanan Informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (*business continuity*), meminimasi resiko bisnis (*reduce business risk*) dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis. Menurut Simanungkalit (2009) keamanan Informasi adalah perlindungan informasi dari berbagai macam ancaman agar menjamin kelanjutan usaha / bisnis, mengurangi resiko bisnis dan meningkatkan return of investment dan peluang bisnis. Keamanan sistem informasi merupakan suatu kegiatperlindungan atau pencegahan terhadap gangguan penyalahgunaan informasi yang dilakukan oleh orang-orang yang tidak bertanggung jawab terhadap jalannya suatu sistem(Supriyatna, 2014).

3.3 ISO/IEC 27001

ISO/IEC 27001 merupakan kerangka kerja yang digunakan untuk menspesifikasikan kebutuhan untuk membangun, menerapkan, mengawasi dan meningkatkan secara berkala pada manajemen orang, proses dan TIK di sebuah organisasi (baik berskala kecil, sedang maupun besar). Kerangka kerja ini bersifat independen terhadap produk TIK (tidak bergantung pada produk tertentu), mensyaratkan penggunaan pendekatan manajemen berbasis resiko, dan dirancang untuk menjamin agar beberapa kontrol keamanan yang digunakan mampu melindungi aset informasi dari berbagai risiko dan memberi keyakinan keamanan bagi pemangku kepentingan. Struktur organisasi ISO/IEC 27001 dibagi dalam dua besar yaitu (Erfina, Utami and Sunyoto, 2018):

1. Klausul (*mandatory process*) merupakan persyaratan yang harus dipenuhi jika organisasi menerapkan Sistem Manajemen Keamanan Informasi menggunakan kerangka kerja ISO/IEC 27001.
2. Annex A (*security control*) merupakan dokumen referensi yang disediakan dan dapat dijadikan rujukan untuk menentukan kontrol keamanan apa yang perlu diterapkan dalam Sistem Manajemen Keamanan Informasi..

3.4 Metode penelitian

Penelitian ini menggunakan metode mix methods atau penelitian campuran antara penelitian kualitatif dan kuantitatif. Jenis penelitian tersebut menurut Sugiyono (2011) adalah metode penelitian dengan mengkombinasikan antara dua metode penelitian sekaligus, kualitatif dan kuantitatif dalam suatu kegiatan

penelitian, sehingga akan diperoleh data yang lebih komprehensif, valid, reliabel, dan objektif (Isnaeni and Kumaidi, 2015).

Penelitian dimulai dengan melakukan identifikasi masalah dengan cara observasi selama 2 bulan. Melakukan wawancara dengan Kepala Bidang Tata Kelola Teknologi Informasi dan Komunikasi) dan Staff bidang Tata kelola teknologi informasi dan komunikasi. Melakukan Dokumentasi dengan cara mencari dan mengumpulkan *evidence* untuk melihat semuaAnnex dan Klausul telah diimplementasikan berdasarkan buku SNI ISO/IEC ISO27001:2013.

Setelah data terkumpul dilakukan analisis dan mengukur tingkat kematangan (*maturity level*) untuk mengetahui bagaimana selama ini organisasi tersebut mengimplementasikan klausul dan annex pada ISO 27001. Instrumen pengukuran *materity level* yang digunakan dijelaskan pada Tabel 1.

Tabel 1 . Skala *Maturity level*

level	Skala Index Maturity	Deskripsi
0 - Non Existent	0% - 18%	Belum terdapat permasalahan-permasalahan yang harus diatasi. Organisasi merasa tidak membutuhkan adanya mekanisme proses keamanan TI. Sehingga tidak ada pengawasan sama sekali.
1 - Initial/ Ad Hoc	19% - 36%	Sudah terdapat bukti bahwa perusahaan mengetahui adanya permasalahan yang harus diatasi. Organisasi juga sudah memiliki inisiatif untuk melakukan keamanan TI namun sifatnya masih non formal.
2 - Repeatable but Intuitive	37% - 54%	Sudah terdapat perencanaan, pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Organisasi memiliki kebiasaan terpola untuk merencanakan keamanan TI yang dilakukan secara berulang namun belum melibatkan dokumen formal.
3 - Defined	56% - 72%	Sudah memiliki proses-proses keamanan TI yang sudah didokumentasikan dengan baik kemudian dikomunikasikan melalui pelatihan. Organisasi juga menyadari perlunya proses keamanan TI sehingga adanya aturan yang menunjukkan untuk organisasi secara rutin melakukan keamanan TI.
4 - Managed and Measurable	73% - 90%	Sudah terdapat proses komputerisasi dengan baik, pengembangan sistem sudah terarah dan dijalankan secara terorganisir. Proses keamanan TI sudah secara formal dilakukan dan secara terus menerus dievaluasi untuk meningkatkan layanan organisasi.
5 - Optimised	91% - 100%	Sudah mengikuti *best practice* yang ditandai dengan adanya proses otomatisasi pada sistem dengan metodologi yang tepat.

Untuk mengetahui tingkat kematangan Klausul dan annex menggunkan rumus *maturity level* pada (1).

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

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).

4. PEMBAHASAN

LAPAN merupakan Lembaga Pemerintah Non Kementerian (LPNK) yang didirikan pada tahun 1963 berdasarkan Keputusan Presiden Nomor 236 Tahun 1963 tentang Lembaga Penerbangan dan Angkasa Luar Nasional. Keputusan Presiden tersebut diperbaharui dan disempurnakan dengan Keputusan Presiden Nomor 103 Tahun 2001 tentang Kedudukan, Tugas, Fungsi, Kewenangan, Susunan Organisasi, dan Tata Kerja Lembaga Pemerintah Non Departemen sebagaimana telah beberapa kali diubah terakhir dengan Peraturan Presiden Nomor 64 Tahun 2005. Keputusan Presiden tersebut kemudian dijabarkan lebih lanjut dengan Peraturan Kepala Lembaga Penerbangan dan Antariksa Nasional Nomor 05 Tahun 2014 tentang Perubahan Atas Peraturan Kepala Lembaga Penerbangan dan Antariksa Nasional Nomor 02 Tahun 2011 Gambar 1.1 Kantor LAPAN Pusat Renstra LAPAN 2015 - 2019 3 tentang Organisasi dan Tata Kerja Lembaga Penerbangan dan Antariksa Nasional (LAPAN). Dengan disahkannya Undang-Undang Republik Indonesia Nomor 21 Tahun

2013 tentang Keantariksaan, dan telah disahkannya Peraturan Presiden no 49 tahun 2015 tentang Lembaga Penerbangan dan Antariksa Nasional yang diundangkan pada lembar negara pada 29 April 2015, maka disusunlah Peraturan Kepala tentang Organisasi dan Tata Kerja LAPAN. Perka no 8 Tahun 2015 tentang Organisasi dan Tata Kerja LAPAN merupakan dasar bagi LAPAN untuk melakukan kegiatan penelitian dan pengembangan Teknologi Penerbangan dan Antariksa(LAPAN, 2016).Analisis ketidaksesuaian penerapan SNI ISO/IEC 27001:2013 pada LAPAN menggunakan *checklist* yang didasarkan atas persyaratan SNI ISO/IEC 27001:2013. Evaluasi dengan melakukan pengamatan terhadap penerapan dokumen dan evindence yang telah disediakan oleh LAPAN. Data yang telah dilakukan pengamatan akan diolah dengan menggunakan tingkat kematangan *(maturity level).*

4.1 Analisis Tingkat Kematangan

Hasil dari tingkat kematangan pada PUSTIKPAN berdasarkan analisis dokumen, wawancara, dan observasi dengan *checklist* sesuai dengan SNI ISO/IEC 27001:2013. Hasil analisis tingkat kematangan dapat ditampilkan pada Tabel 2.

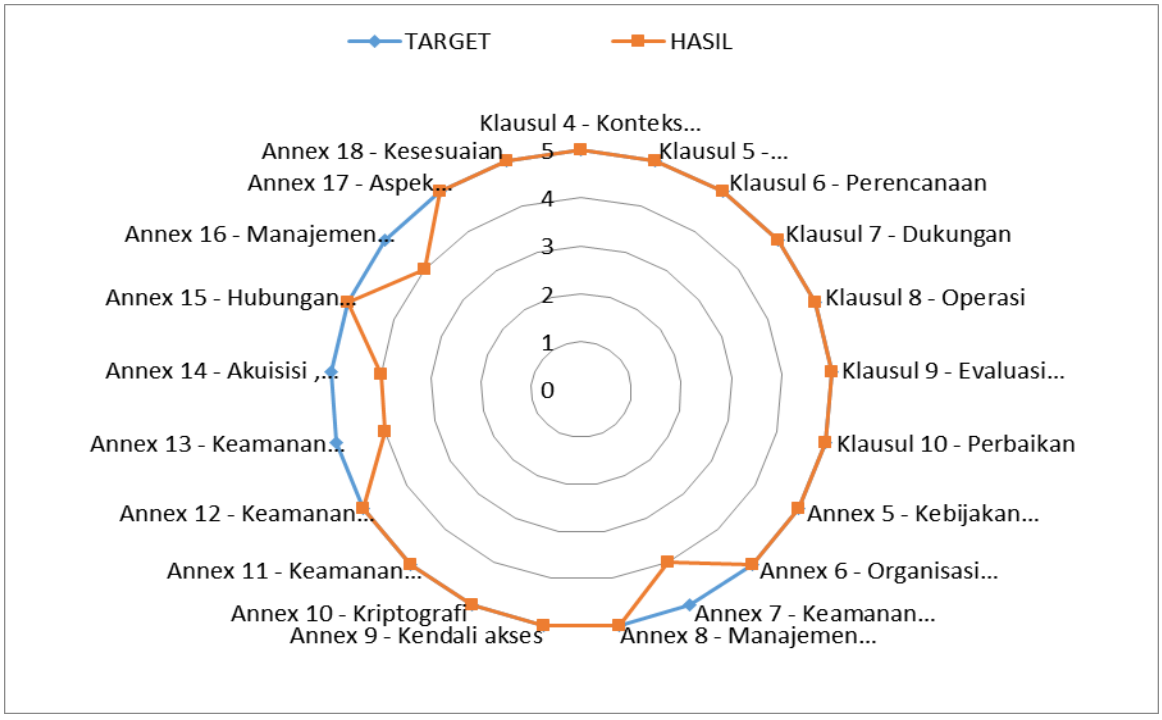
Tabel 2. Hasil Analisis Tingkat Kematangan

Klausul Dan Annex	Target	Hasil
Klausul 4 - Konteks Organisasi	5	5(100%)
Klausul 5 - Kepemimpinan	5	5 (100%)
Klausul 6 - Perencanaan	5	5 (94,12%)
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 (83,33%)
Annex 8 - Manajemen aset	5	5 (91,67%)
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 (85,71%)
Annex 14 - Akuisisi , pengembangan dan perawatan sistem	5	4 (87,50%)
Annex 15 - Hubungan Pemasok	5	5 (100%)
Annex 16 - Manajemen insiden keamanan informasi	5	4 (85,71%)
Annex 17 - Aspek keamanan informasi dari manajemen keberlangsungan bisnis	5	5 (100%)
Annex 18 - Kesesuaian	5	5 (100%)
Total *Maturity Level*		**97,25%**

Pada Table 2 hasil dari analisis tingkat kematangan menggunakan perhitungan persen (%). Klausul 4 mendapatkan hasil 100% berada pada level 5 yaitu *Optimised* yang artinya pada klausul ini sudah berjalan sesuai standar ISO/IEC 27001:2013 dan dokumentasi untuk audit sudah lengkap. Pada Klausul 5 mendapatkan hasil 100% berada pada level 5 yaitu *Optimised* yang artinya pada klausul ini sudah berjalan sesuai standar ISO/IEC 27001:2013 dan dokumentasi untuk audit sudah lengkap. Pada Klausul 6 mendapatkan hasil 94,12% berada pada level 5 yaitu *Optimised* yang artinya pada klausul ini sudah berjalan sesuai standar ISO/IEC 27001:2013 dan dokumentasi untuk audit sudah cukup lengkap namun pada pedoman perlu di revisi pada bagian tabel deskripsi karena tidak ada kolom *risk owner* dan harap di sesuaikan dengan dokumen *risk register*. Pada Klausul 7 mendapatkan hasil 100% berada pada level 5 yaitu *Optimised* yang artinya pada klausul ini sudah berjalan sesuai buku standar ISO/IEC 27001:2013 dan dokumentasi untuk audit sudah lengkap. Pada Klausul 8 mendapatkan hasil 100% berada pada level 5 yaitu *Optimised* yang artinya pada klausul ini sudah berjalan sesuai standar ISO/IEC 27001:2013 dan dokumentasi untuk audit sudah lengkap. Pada Klausul 9 mendapatkan hasil 100% berada pada level 5 yaitu *Optimised* yang artinya pada klausul ini sudah berjalan sesuai standar ISO/IEC 27001:2013 dan dokumentasi untuk audit sudah cukup lengkap namun pada klausul ini dokumen pemantauan dan pengukuran belum ditemukan. Pada Klausul 10 mendapatkan hasil 100% berada pada level 5 yaitu *Optimised* yang artinya pada klausul ini sudah berjalan sesuai sandar ISO/IEC 27001:2013 dan dokumentasi untuk audit sudah lengkap. Pada Annex 5 mendapatkan hasil 100% berada pada level 5 yaitu *Optimised* yang artinya pada annex ini sudah berjalan sesuai dengan standar ISO/IEC 27001:2013 dan dokumentasi untuk audit sudah lengkap. Pada Annex 6 mendapatkan hasil 100% berada pada level 5 yaitu *Optimised* yang artinya pada annex ini sudah berjalan sesuai dengan standar ISO/IEC 27001:2013 dan dokumentasi untuk audit sudah lengkap. Pada Annex 7 mendapatkan hasil 100% berada pada level 4 yaitu

*Managed and Measurable*yang artinya pada annex ini sudah berjalan sesuai dengan standar ISO/IEC 27001:2013 dan dokumentasi untuk audit perlu di cek kembali dalam dokumen kontrak terkait item tanggung jawab kemanan informasi. Pada Annex 8 mendapatkan hasil 91,67% berada pada level 5 yaitu *Optimised* yang artinya pada annex ini sudah berjalan sesuai dengan standar ISO/IEC 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/IEC 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/IEC 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/IEC 27001:2013 namun perlu disediakan lokasi bongkar muat dan dokumentasi untuk audit sudah lengkap. Pada annex 12 mendapatkan hasil 100% berada pada level 5 *Optimised* yang artinya pada annex ini sudah berjalan sesuai dengan standar ISO/IEC 27001:2013 dan dokumentasi sudah lengkap. Pada annex 13 mendapatkan hasil 85,71 berada pada level 4 yaitu *Managed and Measurable* yang artinya pada annex ini sudah berjalan sesuai dengan standar ISO/IEC 27001:2013 dan dokumentasi untuk proses audit sudah lengkap. Pada Annex 14 mendapatkan hasil 87,50% berada pada level 4 yaitu *Managed and Measurable* yang artinya pada annex ini sudah berjalan sesuai dengan standar ISO/IEC 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/IEC 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/IEC 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/IEC 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/IEC 27001:2013 dan dokumentasi untuk audit sudah lengkap. Dapat dilihat bahwa pada Annex 7 memiliki hasil paling rendah yaitu 83,33%. Karena kurangnya dokumen sebagai bukti dari annex tersebut membuat annex tersebut memiliki tingkat kematangan yang rendah.

Hasil rata-rata dari tingkat kematangan ISO/IEC 27001:2013 pada PUSTIKPAN adalah 97,25% dengan level 5 *Optimised* . Secara keseluruhan ISO/IEC 27001:2013 dokumentasi telah dilaksanakan dengan baik hanya perlu ditingkatkan dan dilengkapi kembali mengenai dokumentasi/pengarsipan. *Spider chart* semua kalusul dan annex setelah dianalisis dapat dilihat pada gambar 1.



Gambar 1. *Spider Chart Maturity Level* Klausul dan Annex PUSTIKPAN

5. KESIMPULAN

Berdasarkan hasil audit internal dengan acuan standar ISO/IEC 27001:2013 pada PUSTIKPAN menggunakan perhitungan*maturrity level*, Annex 7 memiliki tingakatan paling rendah diantara Annex lainnyadikarenakan pada dokumen intruksi kerja terkait labeling belum terdaftar dalam dokumen induk sehingga perlu disesuaikan kembali dokumen induknya. Selain itu, masih ada dari klausul dan annex lainnya masih terdapat beberapa dokumen dan formulir yang kurang sesuai antara judul dengan yang tercantum pada kebijakan/prosedur yang ada sehingga kurang adanya sinkronisasi.

Namun secara keseluruhan penggunaan ISO/IEC 27001:2013 telah terlaksana dengan baik karena memiliki rata-rata 97,25% dengan level 5 *Optimised.*Hampir dari seluruh klausul dan annex memenuhi standar ISO/IEC 27001:2013 terlaksana sehingga dari hasil penelitian ini diharapkan PUSTIKPAN dapat meningkatkan kembali dalam pengarsipan dokumen agar memudahkan auditor dalam melakukan audit internal ataupun eksternal serta dapat terlaksananya seluruh kegiatan sesuai dengan standar ISO/IEC 27001:2013.

6. SARAN

Saran untuk peneliti selanjutnya sebaiknya fokus terhadap kontrol keamanan sistem informasi karena masih perlu dimanajemen kembali agar semua aktifitas pengolahan informasi dapat berjalan dengan lancar sesuai prosedur dan dikarenakan ISO belum memiliki metode penilaian khusus maka untuk itu dalam pengembangan penelitian berikutnya dapat menggunakan metode audit lain untuk perbandingan.

7. DAFTAR PUSTAKA

Bakri, M. and Irmayana. N, 2017. Keamanan Informasi SIMHP BPKP Menggunakan Standar ISO 27001, *Jurnal TEKNOKOMPAK*, 11(2), pp. 41–44.

Erfina, Utami and Sunyoto, 2018. Evaluasi Tingkat Kematangan Keamanan Informasi Pada Sistem Informasi Manajemen Universitas Cokroaminoto Palopo, *Jurnal Ilmiah d'Computare*, 8. Available at: journal.uncp.ac.id/index.php/computare/article/view/981.

Indrawati and Hernikawati, 2016. Perancangan Sistem Informasi Manajemen Audit Sistem Elektronik (Simase) Untuk Pelayanan Publik Information System of Electronic System Audit Management (Simase) Design for Public Service, *Jurnal IPTEK-KOM: Jurnal Ilmu Pengetahuan dan Teknologi Komunikasi*, 18(1), pp. 51–68. Available at: https://jurnal.kominfo.go.id/index.php/iptekkom/article/view/51-68.

Isnaeni, W. and Kumaidi. K, 2015. Evaluasi Implementasi PKP Dalam Pembelajaran Biologi di SMAN Kota Semarang Menggunakan Pendekatan Mixed-Method, *Jurnal Penelitian dan Evaluasi Pendidikan*, 19(1), pp. 109–121. doi: 10.21831/pep.v19i1.4561.

Kadir, A, 2014 *Pengenalan Sistem Informasi Edisi Revisi*. Yogyakarta: Andi Offset.

Kusumajaya, R. A., Sembiring, I. and Purnomo. H, 2010. Audit Internal Keamanan Sistem Informasi Keuangan Stekom, pp. 39–44.

LAPAN, 2016. Renstra_Lapan_2015-2019_Rev'.

Ramdhany, T. and Asikin, M. D, 2018. Audit Sistem Informasi Aplikasi Starclick Menggunakan Framework Cobit 4 . 1 Domain Deliver and Support Di Pt . Telekomunikasi Regional Iii Jawa Barat, 11(1).

Santosa and Kuswanto, 2016. Analisa Manajemen Resiko Keamanan Informasi pada Kantor Pelayanan Pajak Pratama XYZ', *Jurnal Ilmiah Rekayasa*, 9, pp. 108–115.

Sidik, Iriani and Yulianto, 2018. Audit Manajemen Keamanan Teknologi Informasi Menggunakan Standar ISO 27001 : 2005 Di PerguruanTinggi XYZ, *MEANS (Media Informasi Analisa dan Sistem)*, 3(2), pp. 99–106. Available at: http://ejournal.ust.ac.id/index.php/Jurnal_Means/.

Supriyatna, A, 2014. Analisis Tingkat Keamanan Sistem Informasi Akademik dengan Mengkombinasikan Standar Bs-7799 dengan SSE-CMM, *Prosiding Seminar Nasional Aplikasi Sains & Teknologi (SNAST)*, (November), pp. 181–188. doi: 10.1002/jcc.23276.

Yuze, Priyadi and Candiwan, 2016. Analisis Sistem Manajemen Keamanan Informasi Menggunakan ISO/IEC 27001 : 2013 Serta Rekomendasi Model Sistem Menggunakan Data Flow Diagram pada Direktorat Sistem Informasi Perguruan Tinggi, *JURNAL SISTEM INFORMASI BISNIS*, 6(1), p. 38. doi: 10.21456/vol6iss1pp38-45.