MJI

Media Jurnal Informatika
Vol. 14, no.1, Juni 2022
http://jurnal.unsur.ac.id/index.php/MJI/index

p-issn : 2088-2114
e-issn : 2477-2542

Penerapan ISO27001 dalam Menjaga dan Meminimalisir Risiko Keamanan Informasi : Literatur Review

Hilaluddin Jauhary[1] , Geta Eldisa Pratiwi[2] , Ariq Zamzami Salim[3] , Fitroh[4]

Program Studi Teknik Informatika[1,2,3,4]
UIN Jakarta[1,2,3,4]
hilaluddin.jauhary19@mhs.uinjkt.ac.id, geta.eldisa19@mhs.uinjkt.ac.id, ariqzamzami.salim19@mhs.uinjkt.ac.id, fitroh@uinjkt.ac.id

Abstract

In Today's Information Security (Information Security) is a very important and critical issue in organizational management. Data security is very important to protect assets or information by providing confidentiality, integrity and availability not only in the telecommunications industry but also in other sectors. This journal aims to minimize the existence of hacking a system by emphasizing the ISO27001 standard policy. The research procedure focuses on the dimensions of ISO27001, Data Security, ISMS, Risk Management. The studies selected from the main database are Scopus. The method or stages used in this journal are using Publish or Perish 7, Mendeley, Zotero, and Microsoft Excel. The selection process was carried out using Microsoft Excel and involved searching for literature sources and screening and screening studies based on titles, abstracts, and full text readings. 13 documents were finally selected and adopted in this journal. Based on the selected journals, it was identified that there are 11 areas that discuss ISO27001 related to data security.

Keywords: ISO27001, Data Security, ISMS (Information Security Manaagement System), Risk Management

Abstrak

Di Masa Sekarang Keamanan data (*Data Security*) menjadi isu yang sangat penting dan kritis dalam manajemen organisasi. Keamanan data sangat penting untuk melindungi aset atau informasi dengan memberikan kerahasiaan, integritas, dan ketersediaannya tidak hanya di industri telekomunikasi tetapi juga di sektor lain. Jurnal ini bertujuan untukmeminimalisir adanya peretasan suatu sistem dengan menekankan kebijakan standar *ISO 27001*. Prosedur penelitian berfokus pada dimensi *ISO27001, Data Security, ISMS, Risk Management.* Studi yang dipilih dari database utama yakniScopus. Metode atau tahapan yang digunakan pada jurnal ini yaitu menggunakan *Publish or Perish 7*, *Mendeley, Zotero,VOSViewer* dan *Microsoft Excel*. Proses seleksi dilakukan menggunakan *Microsoft Excel* dengan melibatkan pencariansumber literatur dan penyaringan dan penyaringan studi berdasarkan judul, abstrak, dan bacaan teks lengkap. 13 dokumen akhirnya dipilih dan diadopsi dalam jurnal ini. Berdasarkan jurnal yang sudah dipilih, diidentifikasi bahwa ada11 jurnal yang membahas terkait ISO27001 dengan keamanan data

.

Kata kunci: *ISO27001,* Keamanan Informasi,*ISMS (Information Security Manaagement System), Management Risiko*

I. PENDAHULUAN

Di era mendatang, keamanan data adalah salah satu yang paling aset penting bagi industri TI. Penilaian Risiko adalah salah satu solusi untuk mencegah data dari pencurian data dan untuk mengenali lubang lingkaran dalam organisasi yang dapat menyebabkan keamanan pelanggaran. Harus ada seperangkat prosedur yang tepat dan kebijakan yang diterapkan untuk mencegah pelanggaran keamanan ini masuk ke organisasi.

Salah satu kerangka kerja yang meliputi Penilaian Risiko adalah Standar ISO 27001 yang berhubungan dengan keamanan organisasi secara keseluruhan. Standar ini dimulai dari menentukan ruang lingkup organisasi hingga sertifikasi dari Standar, meskipun tidak wajib bahwa organisasi harus disertifikasi jika organisasi tersebut mengikuti kebijakan dan kontrol wajib untuk mendapatkan objektif. Standar ISO 27001 digunakan untuk mengimplementasikan Sistem Manajemen Keamanan Informasi (SMKI) di organisasi. Karena sebagian besar keamanan efek tertinggi pelanggaran berasal dari karyawan yang bekerja di organisasi, harus ada pelatihan yang tepat dalam organisasi untuk melindungi sistem agar tidak disusupi secara internal, program penyadaran harus dilakukan untuk karyawan dan staf sehingga keamanan informasi kelangsungan bisnis tidak secara eksklusif tergantung pada kehadiran individu tertentu yang dapat menyebabkan sistem berhenti/rusak tergantung pada aksesibilitas tertentu para karyawan. Sistem Manajemen Keamanan Informasi (SMKI) memberikan solusi lengkap untuk informasi yang unggul pertemuan keamanan dengan menyediakan prosedur yang diperlukan, alat, dan langkah-langkah untuk meningkatkan dan memelihara organisasi informasi

yang dilindungi. Para karyawan dan staf organisasi harus diberikan kesadaran yang tepat dan pelatihan tentang Standar ISO dan mengapa itu penting ke organisasi mereka. Setelah sesuai dengan ISO 27001, organisasi dapat memberikan jaminan kepada klien dan mitra merekabahwa data mereka aman di dalam organisasi.

1.1.Landasan Teori

1.1.1. ISO 27001

ISO/IEC 27001 merupakan salah satu metode dengan standard keamanan informasi yang diterbitkan *International Organization for Standarization dan International Electrotecnical Comission* (Utomo & Affandy, 2012). ISO 27001 menjadi standar manajemen keamanan informasi yang luas digunakan oleh bisnis dan organisasi, menyediakan referensi tertentu yang paling komprehensif untuk menajemen keamanan informasi di dunia.

Selanjutnya, ISO 27001 juga didefinisikansebagai dokumen standar sistem manajemen keamanan informasi atau *Information Security Management System*, biasa disebut *ISMS*, yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah institusi dalam usaha mereka untuk mengevaluasi, mengimplementasikan, dan memelihara keamanan informasi berdasarkan "*best practice*" dalam pengamanan informasi (Syafrizal & Kom, 2009). ISO 27001 berfokus pada pengurangan risiko terhadap informasi yang bernilai bagi organisasi (Ramadhani et al. 2018). Ada 11 klausul pada ISO 27001, yaitu kebijakan keamanan informasi, organisasi keamanan informasi, pengelolaan aset, kesesuaian, keamanan sumber daya manusia, keamanan fisik dan lingkungan, akses kontrol, akuisisi, pengembangan, dan pemeliharaan sistem informasi, manajemen komunikasi dan operasi, manajemen insiden keamanan informasi, dan manajemen kelangsungan bisnis (Utomo & Affandi, 2012). Koldo Peciña dan dkk. menggunakan dua teknik yaitu ISO 31000 dan ISO 27001 yang menghasilkan evaluasi keamanan fisik dan logis. Satu-satunya batasan adalah bahwa tidak ada manajemen keamanan yang diterapkan untuk memastikan perlindungan semua aset. [1]. Carol Hsu dan dkk. membandingkan daftar perusahaan dengan dan tanpa sertifikasi ISO 27001 dengan kinerja mereka. Hanya informasi keuangan yang tidak tersedia di perusahaan manapun [2]. Manar Abu Thalib dan dkk. memberikan pentingnya prosedur ISO 27001 untuk dijalankan dalam sebuah manajemen keamanan informasi. Ruang lingkup masa depan adalah untuk mengevaluasi kursus Keamanan Informasi yang diperkaya, dan meningkatkan Teknologi Keamanan Informasi [3]. Elvi Fetrina dan dkk. Pengumpulan data dilakukan dengan wawancara dan studi pustaka. Hasil dari surveiini adalah informasi manajemen persediaan. Mereka menggunakan *Rapid Application Development dan Object Oriented Approach* menggunakan bahasa *Unified Modeling*. Masalah mengenai kemungkinan Data Hilang atau rusak muncul dalam hal ini pada saat pelaksanaan [4]. Awni Itradat dan dkk. menggunakan ISO 27001 yang menjamin lingkungan yang paling terlindungi untuk organisasi. Satu-satunya batasan muncul bahwa tim yang mengimplementasikan harus memiliki semua pengetahuan tentang Standar ISO 27001 [5]. Yogesh Verma dan dkk. menyoroti desain dan pengembangan sistem manajemen aset perangkatlunak terpusat berbasis web, mengurangi biaya pengembangan secara keseluruhan, dan meningkatkan nilai dan efisiensi perangkat lunak. Keterbatasannya adalah tidak adanya monitoring dan evaluasi untuk mekanisme umpan balik yang dibangun secara berkala menuju perbaikan berkelanjutan [6]. Martin Jakubicka, menyelidiki desain Manajemen Aset Perangkat Lunak yang dibuat untuk tujuan Universitas dan membahas masalah yang paling penting dalam situasi ini. Satu-satunya batasan adalah bahwa tidak ada metodologi yang sesuai untuk membuat SAM. Afifah Muftinisa dan dkk. menggunakan teknik yang mengelola sumber daya mereka, memelihara catatan aset rinci serta menjaga kondisi aset. Keterbatasannyaadalah tidak banyak aset fleksibel. Thomson Martin menggunakan sejumlah cara di mana SAM dapat membantu organisasi untuk menjaga aset tetap aman, tetapi itu membutuhkan banyak memelihara catatan aset secara rinci serta menjaga kondisi aset. Keterbatasannya adalah tidak banyak aset fleksibel. Thomson Martin menggunakan sejumlah cara di mana SAM dapat membantu organisasi untuk menjaga aset tetap aman, tetapi itu membutuhkan banyak memelihara catatan aset secara rinci serta menjaga kondisi aset. Keterbatasannya adalah tidak banyak aset fleksibel [7]. Thomson Martin menggunakan sejumlahcara di mana SAM dapat membantu organisasi untuk menjaga aset tetap aman, tetapi itu membutuhkan banyak

Tujuan audit internal untuk standar ISO 27001 adalah memahami praktik pemeriksaan sistem manajemen keamanan informasi. Ruang lingkup audit termasuk penilaian layanan keamanan informasi, formulir, dan kontrol yang digambarkan dalam dokumentasi SMKI untuk mengamankan privasi, keandalan, dan aksesibilitas aset informasi penting kota di dalam cakupan SMKI. Daftar dua puluh sumber informasi diberikan pada awal audit sebagai inventaris untuk dipertimbangkan dalam lingkup SMKI (Sistem Manajemen Keamanan Informasi).

Gambar 1 : Manfaat ISO 27001

1.1.2. Information Security

Pentingnya sebuah informasi menimbulkan munculnya istilah keamanan informasi. Saat ini sema- kin banyak sumber informasi yang berasal dari internet sehingga keamanan informasi menyangkut teknologi komputer dan jaringan serta informasi dan komunikasi. Tujuan dari keamanan informasi adalah untuk menjaga keberlangsungan bisnis dan mengurangi adanya penu- runan nilai bisnis dengan membatasi efek dari insiden keamanan. Kemudian menurut Siponen dan Oinas Kukkonen, tujuan dari keamanan [8] informasi adalah untuk kerahasiaan, integritas, ketersediaan, dan tidak adanya penolakan informasi. Sumber informasi meru- pakan asset yang harus selalu dijaga keamanannya agar tidak disalahgunakan oleh pihak tertentu.[9]

Tinjauan keamanan informasi menurut Whitman dan Mattod [10] digambarkan sebagai berikut:

Gambar 2 : Tinjauan Keamanan Informasi

a. *Physical Security*, berfokus pada strategi untuk mengamankan hal yang bersifat fisik seperti asset fisik pemerintah atau organisasi, karyawan dan pegawai, danlokasi bekerja dari ancaman musi- bah, bencana alam, atau tindakan akses tanpa izin.
b. *Personal Security*, berkaitan dengan physical securi- ty dalam melindungi organisasi dan orang-orang didalamnya baik organisasi pemerintah maupun swasta.
c. *Operation Security*, berfokus pada strategi opera- sional untuk mengamankan organisasi pemerintah atau swasta agar dapat bekerjatanpa gangguan.
d. *Communication Security*, mengamankanmedia komunikasi, teknologi komunikasi, dan meman- faatkan peralatan teknologikomunikasi untuk mencapai tujuanorganisasi.
e. *Network Security*, berkaitan dengan pengamanan pada sumber data organisasi, jaringan dan isinya, serta kemampuan untuk menggunakan jaringan dan data tersebut untuk komunikasi data dalam or- ganisasi.

1.1.3. Manajemen Risiko

Menurut Fahmi (2010) manajemen risiko adalah satu disiplin ilmu yang mempelajari tentang tindakan-tindakan organisasi dalam mengatasi masalah berbasis manajemen yang sistematis dan menyeluruh. Djojo Soedarso (2003) memiliki pandangan yang berbeda. Menurutnya manajemen risiko adalah penerapan fungsi manajemen secara umum untuk memetakan masalah dan solusinya yang terjadi di dalam sebuah organisasi perusahaan maupun keluarga dan masyarakat. Sedangkan menurut Tampubulon (2004) manajemen risiko adalah satu proses yang dilakukan untuk mengakomodasi segala kemungkinan buruk dari sebuah transaksi bisnis.

Manajemen risiko memiliki komponen-komponen tertentu yang membedakannya dengan manajemen bisnis lain. Instrumen inilah yang harus ada di dalam manajemen baru proses pelaksanaannya bisa dilakukan dengan maksimal. Ini dia komponen yang dimaksud:

1. Lingkungan Internal

Lingkungan internal maksudnya adalahsegala risiko yang kemungkinan terjadi di dalam internal perusahaan. Di dalam komponen ini, tidakada deteksi terhadap risiko yang terjadi antara perusahaan dengan faktor luar seperti pelanggan, klien dan semacamnya. Sekalipun kadang efek risiko internal ini juga berimbas pada hal tersebut. Komponen lingkungan internal dalam manajemen risiko terkait dengan kedisiplinan karyawan, etika bekerja, Kompetensi pegawai, tingkat kesejahteraan bawahan dan selainnya. Ini perlu juga dilakukan deteksi manajemen untuk mencegahmunculnya risiko dari kriteria tersebut.

2. Penentuan Sasaran

Penentuan sasaran maksudnya adalah pihak perusahaan harus memasukkan sasaran risiko yangjelas yang akan coba diselesaikan melalui sistem manajemen. Di dalamnya biasanya tercakup dua hal yaitu risiko yang muncul dari statemen visi danmisi usaha serta sasaran risiko yang datang dari kegiatan teknis atau operasional. Tidak dimungkiri setiap perusahaan pasti memiliki visi

dan misi usaha. Namun terkadang apa yang diidamkan tersebut tidak sesuai dengan harapan.

3. Identifikasi Peristiwa

Komponen manajemen risiko yang ketiga adalah identifikasi peristiwa. Maksudnya adalahtidak disebutkan manajemen risiko jika pihak perusahaan tidak memiliki data detail hasil identifikasi peristiwa. Seharusnya ini memang sudah didapatkan sebelum usaha mulai dijalankan.

4. Penilaian Risiko

Memungkinkan sebuah organisasi perusahaan ataupun bisnis untuk menilai sebuah kejadian atau keadaan dan kaitannya dengan pencapaian tujuan perusahaan atau bisnis tersebut.Manajemen perlu melakukan analisis mengenai dampak yang mungkin terjadi akibat resiko dengan 2 perspektif, yaitu : *Likelihood* (kecenderungan/peluang), *Impact/consequence*(besaran dari realisasi risiko).

5.Tanggapan Risiko

Selain melakukan penilaian terhadap risiko, juga menentukan tanggapan atau respon terhadap risiko tersebut. Respon dari manajemen tergantungrisiko apa yang dihadapi. Respon atau tanggapan tersebut bisa dalam bentuk :

a. Menghindari risiko (*avoidance*
b. Mengurangi risiko (*reduction*)
c. Memindahkan risiko (*sharing*)
d. Menerima risiko (*acceptance*)
e. Aktivitas Pengendalian

6.Pemantauan (*Monitoring*)

Monitoring adalah komponen terakhir dalam manajemen risiko. Proses pemantauan dilakukan secara terus menerus untuk memastikan setiap komponen lainnya berfungsi sebagaimana mestinya. Hal penting yang perlu diperhatikan dalam proses monitoring adalah pelaporan yang tidak lengkap atau berlebihan.

II.METODOLOGI PENELITIAN

Metode penelitian yang digunakan pada penelitian ini adalah studi literatur. Menurut (M. Zed)[11] metode studi literatur adalah serangkaian kegiatan yang berkenaan dengan metode pengumpulan dari berbagai data pustaka, seperti jurnal, buku, *website* ataupun sumber lainnya, kemudian membaca dan mencatat serta melakukan pengolahan bahan penelitian terkait. Menurut (M. Nazir and R. Sikmumbang)[12] menyatakan bahwa studi literatur adalah sebuah metode yang dilakukan dengan menelaah secara tekun akan kepustakaan yangdiperlukan dalam penelitian..

III.HASIL PENELITIAN

Langkah pertama yaitu, peneliti menggunakan alat bantu atau tools, yaitu *Publish or Perish 7*. *Publish or Perish* adalah sebuah software program yang digunakan untuk menganalisa dan mendapatkan kembali sitasi akademik dari beberapa sumber seperti, *Google Scholar, Scopus, Microsoft Academic Search*, dll (A.-W. Harzing)[13]. Dalam penelitian ini, peneliti mencari paper yang mengandung judul "ISO 27001" dari sumber *Scopus* dan didapatkan 500 paper yang terbagi dari 315 buku dan 185 jurnal atau artikel. Peneliti hanya memakaki 185 jurnal tersebut.

Langkah kedua, yaitu data dari *Publish or Perish 7* disimpan dalam format .ris (*RIS/Ref Manager*) dan kemudian di import kedalam *Mendeley* untuk mendapatkan rincian paper tersebut. *Mendeley* adalah sebuah perangkat lunak yang digunakan untuk mengintegrasikan "*citation & reference manager*" ke dalam sebuah jejaring sosial. Dengan jejaring semacam ini, peneliti di berbagai belahan dunia dapat berkolaborasi dan melakukan sharing data penelitian (H. Supriyanto)[14]. Setelah melakukan *import*, peneliti melakukan sinkronisasi di *Mendeley* agar jumlah data dari 185 jurnal tersebut dapat otomatis diperbaharui.

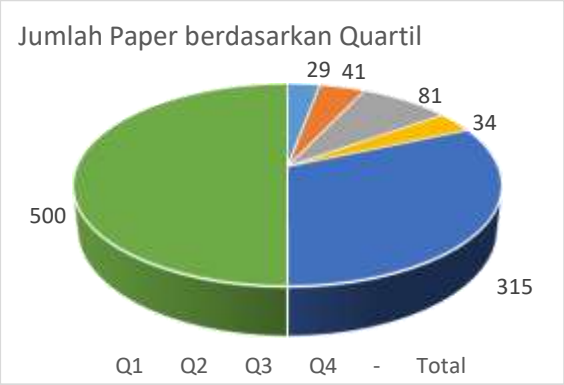
Langkah ketiga, yaitu menyimpan data yangtelah disinkronkan di *Mendeley* ke dalam format .csv (*Comma Separated Value*s) agar dapat diimport di *Microsoft Excel*. Setelah data di import ke *Microsoft Excel*, peneliti melakukan penyaringan data dengan menyesuaikan topik penelitian. Karena sumber data berasal dari *Scopus*, peneliti melakukan penyaringan data dengan bantuan masterscopus, artinya jurnal yang dikenali adalah jurnal yang telah terindeks *Scopus*. Data masterscopus (Scimago)[15] di import dalam sheet yang berbeda di file *Microsoft Excel* yangsama dengan data *Mendeley* sebelumnya.

Langkah keempat adalah penyaringan dengan *master Scopus*. Dalam tahap ini jurnal-jurnal yang terindeks maupun tidak terindeks *Scopus* dibagi dalam 4 Kuartil (*Q-ranking of journal*) dimana Q1 merupakan ranking tertinggi dan Q4 adalah ranking terendah. Kuartil ini adalah kategori jurnal ilmiah yang mewakili tingkat kutipan yang diidentifikasi oleh indikatorscientometric. Jadi, publikasi berkisar dari yang paling direferensikan. Dari 185 jurnal yang didapatkan, untuk Q1 dan Q2 masing-masing hanya berjumlah 29 jurnal dan 41 jurnal. Dan untuk Q3 dan Q4 masing masing 81dan 34 jurnal. Dan kami berfokus pada *keyword* ISO 27001 dalam rentang tahun 0-2021. Dan kami memutuskan untuk memakai jurnal 5 tahun terakhir yaitu 2016-2021.

Tabel 1 : Sortir Jurnal Berdasarkan Quartil

No	Quartile	Jumlah
1	Q1	29
2	Q2	41
3	Q3	81
4	Q4	34
5	-	315
Total		500

No DOI : 10.35194/mji.v%vi%i.1581



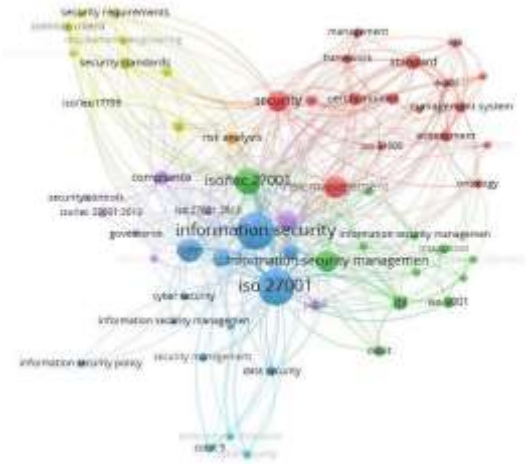
Gambar 3 : Diagram Klasifikasi Jurnal BerdasarkanQuartil

Dapat dilihat dalam Gambar 3 merupakan hasil penyaringan data dengan *masterscopus* yang sudah terbagi dalam Q1-Q4 , dan ada 315 jurnal yang tidak terindeks *Scopus*.

Langkah kelima adalah penyaringan lanjutan berdasarkan tahun terbit. Dalam Gambar 4, dapat terlihat rincian jumlah jurnal yang diterbitkan di *Scopus* berdasarkan tahun terbit nya seperti berikut

Gambar 4 : Klarifikasi Jurnal Per tahun

Dari hasil tersebut, kami membatasi jurnal dengan ketentuan rentang tahun 2016-2021 serta kata kunci ISO27001, *Information Security* dan *Risk Management*berdasarkan klaster dari *VOSviewer*



Gambar 5 *VOSViewer* Jurnal *Keyword* ISO27001

IV. PEMBAHASAN

No	Tittle	Author
1.	Best practices of auditing in an organization using ISO 27001 standard	Phirke, Amogh; Ghorpade-Aher, Jayshree (2019)
2.	Adopting an ISO/IEC 27005:2011-based risk treatment plan to prevent patients from data theft	Hamit, Laura Cassandra; Sarkan, Haslina Md; Mohd Azmi, Nurulhuda Firdaus; Mahrin, Mohd Naz ri; Chuprat, Suriayati; Yahya, Yazriwati (2020)
3.	Readiness of Information Security Management Systems (ISMS) policy on hospital staff using epatuh system	Ismail, Waidah; Alwi, Najwa Haayati Mohd; Ismail, Roesnita; Bahari, Mahadi; Zakaria, Omar (2018)
4.	Analysis of factors that inhibiting implementation of Information Security Management System (ISMS) based on ISO 27001	Tatiara, R.; Fajar, A. N.; Siregar, B.; Gunawan, W. (2018)
5.	*ISO/IEC 27001 implementation in SMEs: Investigation on management of information assets*	Muthaiyah, Saravanan; Zaw, Thein Oak Kyaw (2018)

6.	*Integration of ITIL V3, ISO 20000 & iso 27001:2013forit services and security management system*	Faruq, Barra Al; Herlianto, Hemdani Rahendra; Simbolon, Siharparulian Hendrik; Utama, Ditdit Nugeraha; Wibowo, Antoni (2020)
7.	*Implementation of an Information Security Management System Based on the ISO/IEC27001: 2013 Standardfor the Information Technology Division*	Aquino Cruz, Mario; Huallpa Laguna, Jessica Noralinda; Huillcen Baca, Herwin Alayn; Carpio Vargas, Edgar Eloy; Palomino Valdivia, Flor de Luz(2021)
8.	*Measuring information security and cybersecurity onprivate cloud computing*	Wendy; Wang, Gunawan (2019)
9.	*Risk based thinking – New approach for modernenterprises' management*	Pacaiova, Hana; Nagyova, Anna (2019)
10.	*Aggregating corporate information security maturity levels of different assets*	Schmid, Michael; Pape, Sebastian (2020)

Dari tabel jurnal di atas kita akan membahas masing masing hasil penelitian dari jurnal tersebut.

Pertama pada penelitian Dalam beberapa tahun terakhir dengan penggunaan intensif teknologi informasi, keamanan data telah berubah menjadi isu kritis dan penting dalam manajemen organisasi. Berbagai Standar dan aturan yang ada untuk keamanan Informasi, misalnya, ISO/IEC 27001, ISO/IEC 27002. Namun, organisasi menghadapi tantangan yang berbeda untuk menerapkan standar. Dalam makalah ini, kami menyajikan status proses eksekusi ISO/IEC 27001 di Perusahaan Kecil dan Menengah. Dengan menerapkan ISO 27001, organisasi mendapat kesempatan untuk membuktikan keaslian dan menunjukkan kepada klien bahwa organisasi bekerja sesuai dengan praktik terbaik yang diakui. Ini membantu organisasi "*IKSC Knowledge Bridge Pvt Ltd."* dalam mengurangi biaya, risiko, dan meningkatkan nilai merek. Hasil yang diperoleh menyimpulkan tidak hanya kebutuhan untuk memikirkan aspek teknis, hukum organisasi, tetapi juga yang terkait dengan orang-orang seperti pelatihan, pengetahuan, menciptakan kesadaran, untuk mencapai manajemen keamanan informasi yang sukses. [16]

Keamanan informasi merupakan topik penting yang memberikan kontribusi keberhasilan operasi bisnis saat ini. Urgensi penerapan keamanan informasi yang efektif dapat dilihat di semua entitas bisnis dan nirlaba. Pada penelitian mengambil kasus universitas XYZ yang menggunakan komputasi awan pribadi sebagai alat penting untuk mendukung proses bisnisnya. Penelitian ini membahas cara efektif mengukur tingkat keamanan informasi dan kinerja *CyberSecurity* yang berfokus pada penggunaan cloud pribadi dengan rekomendasinya. Artikel tersebut menerapkan kerangka kerja ISO 27001:2013 dengan melibatkan semua klausul dalam Lampiran ISO 27001:2013 untuk *CyberSecurity*, bagian Menerapkan *CyberSecurity*. Lampiran ISO 27001:2013 untuk *CyberSecurity* digunakan masing-masing untuk mengukur keamanan informasi dan kinerja *CyberSecurity*. [17]

V.KESIMPULAN

Berdasarkan pembahasan studi literatur dari jurnal-jurnal tersebut terdapat beberapa hal yang dapat disimpulkan bahwa ISO 27001 atau merupakan suatu hal yang penting. Karena ISO 27001 bertujuan untuk meningkatkan keamanan dan integritas suatu perusahaan secara keseluruhan. ISO 27001 juga digunakan untuk mencapai tujuan perusahaan demi mencapai investasi terbaik dalam bidang sistem informasi dan teknologi. Maka dari itu perusahaan bertanggung jawab untuk memberikan layanan TI yang baik dan menjaga keamanan TI untuk meningkatkan keunggulan kompetitif mereka Keamanan TI dan layanan TI memiliki standar dan kerangka kerja internasional mereka sendiri. Ketika sistem manajemen layanan TI (SMS) dan sistem manajemen keamanan informasi (ISMS) diimplementasikan secara terpisah, dapat menyebabkan konsumsi sumber daya yang tinggi dan mahal [18] sehingga ISO 27001 dapat dijadikan sebagai suatu standar atau panduan untuk membantu mengelola suatu perusahaan mencapai tujuannya yaitu dengan memanfaatkan TI. ISO 27001 juga memberikan panduan kerangka kerja atau framework yang dapat mengendalikan seluruh kegiatan keamananan dan integritas secara detail dan juga jelas sehingga dapat membantu memudahkan pengambilan keputusan di level atas dalam organisasi.

VI. REFERENSI

[1] Amogh Phirke , Prof. Jayshree Ghorpade-Aher, "Penilaian Risiko Kepatuhan Perangkat Lunak menggunakan Standar ISO 27001", JASC: Journal of Applied Science and Computations, Volume 6 Issue 3, March 2019

[2] Koldo Pecia, Ricardo Estremera, Alfonso Bilbao, Enrique Bilbao, "Model Organisasi Manajemen Keamanan Fisik dan Logis

Berdasarkan ISO 31000 dan ISO 27001", Konferensi IEEE Carnahan tentang Teknologi Keamanan, 1821Oktober 2011

[3] Carol Hsu, Tawei Wang, Ang Lu, "Dampak Sertifikasi ISO 27001 pada Kinerja Perusahaan", IEEE, 2016 Konferensi Internasional Hawaii ke-49 tentang Ilmu Sistem (HICSS), 5-8 Januari 2016

[4] Manar Abu Thalib, Adel Khelifi, Tahsin Ugurlu, "Using ISO 27001 in Teaching Information Security", IEEE, IECON 2012 - Konferensi Tahunan ke-38 tentang Masyarakat Elektronik Industri IEEE, 25- 28 Oktober 2012

[5] Elvi Fetrina, Eri Rustamaji, Tatat Nuraeni , Yusuf Durrachman, "Pengembangan Sistem Informasi Manajemen Persediaan di Bprtik Kemkominfo Jakarta", IEEE 5th International Conference on Cyber and IT Service Management (CITSM), 8-10Agustus 2017

[6] Awni Itradat, Sari Sultan, Maram Al-Junaidi, Rawa'a Qaffaf, Feda'a Mashal, dan Fatima Daas, "Mengembangkan Sistem Manajemen Keamanan Informasi ISO 27001 untuk Lembaga Pendidikan: Universitas Hashemite sebagai Studi Kasus", JJMIE (Yordania Jurnal Teknik Mesin dan Industri)
ISSN 1995-6665 Volume 8, April. 2014

[7] Yogesh Verma, R. Nandakumar, "Pengembangan Sistem Manajemen Aset Perangkat Lunak untuk Memfasilitasi Penggunaan Kembali Perangkat Lunak", Konferensi Internasional IET (Institusi Teknik dan Teknologi) tentang Rekayasa Perangkat Lunak dan Pemodelan dan Pengembangan Aplikasi Seluler (ICSEMA 2012), 19-21 Desember 2012

[8] Eka Fuji Astuti and Puspita Kencana Sari, 'Analisis Budaya Keamanan Informasi Di Klinik Pratama Kota Bandung', Jurnal Mitra Manajemen, 2019.

[9] Christian Sillaber, Andrea Mussmann, and Ruth Breu, 'Experience: Data and Information Quality Challenges in Governance, Risk, and Compliance Management', Journal of Data and Information Quality, 11.2 (2019)https://dl.acm.org/doi/10.1145/3297721

[10] Tridib Bandyopadhyay and Humayun Zafar, 'Influence of Information Overload on It Security Behavior: A Theoretical Framework', in AMCIS 2017 - America's Conference on Information Systems: A Tradition of Innovation, 2017

[11] M. Zed, Metode Penelitian Kepustakaan. Jakarta: Yayasan Pustaka Obor Indonesia, 2014.

[12] M. Nazir and R. Sikmumbang, Metode Penelitian. Bogor: Ghalia Indonesia, 2009.

[13] A.-W. Harzing, "About Publish or Perish," 2016. https://harzing.com/resources/publish-or-perish (accessed Jun. 18, 2021).

[14] H. Supriyanto, "Pengantar & Instalasi Mendeley."http://lib.ugm.ac.id/ind/?page_id=336.

[15] Scimago, "Journal Rankings on Scopus," 2021. https://www.scimagojr.com/journalrank.php (accessed Jun. 18, 2021).

[16] Phirke, Amogh; Ghorpade-Aher, Jayshree Best practices of auditing in an organization using ISO 27001 standard. 2019

[17] Wendy; Wang, Gunawan Measuring information security and cybersecurity on private cloud computing, 2019

[18] Faruq, Barra Al; Herlianto, Hemdani Rahendra; Simbolon, Siharparulian Hendrik; Utama, Ditdit Nugeraha; Wibowo, Antoni Integration of ITIL V3, ISO 20000 & iso 27001:2013forit services and security management system. 2020