Online : ejournal.stmikbinapatria.ac.id/index.php/JT/issue/ ISSBN : 1978-5569

METODE SILOGISME *AND* UNTUK VALIDITAS JAWABAN DARI RESPONDEN DALAM ANALISIS *MATURITY LEVEL* KEAMANAN INFORMASI BERBASIS SNI ISO 27001:2013 PADA DINAS KEPENDUDUKAN DAN PENCATATAN SIPIL KOTA XYZ

Haries Anom Suseyto Aji Nugroho[1)], **Wing Wahyu Winarno**[2)], **Sudarmawan**[3)]
[1)] *"Magister Teknik Informatika" UNIVERSITAS AMIKOM Yogyakarta*
[2)] *STIE YKPN Yogyakarta*
[3)] *UNIVERSITAS AMIKOM Yogyakarta*
Email : anom.haries@gmail.com [1)], wingwahyuwinarno@gmail.com [2)], *sudarmawan@amikom.ac.id* [3)]

Abstract

Various threats that attack data and information from organizations are increasing such as malware attacks, hackers, and natural disasters. If the threats of such information are not addressed immediately, it will result in the risk of loss of data, information along with its infrastructure on aspects of confidentiality, integrity, and availability. As a result, the organization's business processes will be temporarily suspended and may even lead to the destruction of an organization. One method of preventing and minimizing information security threats is the Maturity Level method. The method serves to measure the level of maturity of the application of information security in the organization. Maturity Level method is a very appropriate method if used to measure how mature organization in information security management that can finally provide recommendations to improve the security of information in accordance with the needs of the organization but depends on the data obtained when implementing the data identification process. Many methods are used to ensure that the data provided by the respondents is guaranteed to be valid as the observation method. The weakness of observation method is not all respondents will want to show information suppose information contained in information assets due to several reasons such as regulation of the limits of safe areas.

Keywords**:**Threat, Method, Maturity Level, AND Syllogism, Clause

Abstrak

Berbagai ancaman yang menyerang data dan informasi dari organisasi kian marak terjadi seperti serangan *malware*, *hacker* dan bencana alam. Jika ancaman-ancaman dari informasi tersebut tidak segera ditanggulangi, maka akan menimbulkan risiko hilangnya data, informasi berserta infrastrukturnya pada aspek *confidentiality*, *integrity* dan *availability*. Akibatnya proses bisnis organisasi akan terhenti baik untuk sementara waktu bahkan dapat menyebabkan kehancuran sebuah organisasi. Salah satu metode dalam mencegah dan meminimalisir ancaman keamanan informasi adalah metode *Maturity Level*. Metode tersebut berfungsi mengukur tingkat kematangan dari penerapan keamanan informasi pada organisasi. Metode *Maturity Level* adalah metode yang sangat tepat jika digunakan untuk mengukur seberapa matang organisasi dalam memanajemen keamanan informasi yang akhirnya dapat memberikan rekomendasi untuk meningkatkan keamanan informasi sesuai dengan kebutuhan organisasi akan tetapi tergantung dengan data yang didapatkan ketika melaksanakan proses identifikasi data. Banyak metode yang digunakan agar data yang diberikan responden terjamin kevalidannya seperti metode observasi. Kelemahan metode observasi adalah tidak semua responden akan mau menunjukkan informasi

misalkan informasi yang terkandung dalam aset informasi dikarenakan beberapa sebab seperti regulasi batasan daerah aman dan lain sebagainya.

Kata kunci: **Ancaman, Metode, *Maturity Level*, Metode Silogisme *AND*, Klausul**

1. Pendahuluan

Maturity Level adalah sebuah metode yang digunakan untuk mengukur tingkat kedewasaan penerapan keamanan informasi yang ada pada organisasi. Sarno (2000), menyatakan bahwa *maturity level* berfungsi sebagai evaluasi kondisi sekarang dari organisasi untuk menjamin bahwa perbaikan proses pengolahan TI secara kontinyu dapat dilaksanakan. Pada penelitian ini *maturity level* digunakan untuk mengidentifikasi apakah organisasi sudah mempunyai dan menerapkan kebijakan keamanan informasi.

Berbagai ancaman yang menyerang data dan informasi dari organisasi kian marak terjadi. Seperti virus *WannaCry* yang telah menyerang 17 Perusahaan di Korea Selatan (Pratiwi, D., 2017). Virus tersebut adalah virus yang mempunyai fungsi untuk mengunci data-data yang ada pada komputer. Malware jenis ransomeware yang sempat beredar di Indonesia bahkan sampai melumpuhkan server di perusahaan minyak terbesar di Rusia, mengganggu operasi bank Ukraina dan mematikan komputer di perusahaan perkapalan dan periklanan multinasional (Editor, 2017).

Hacker juga mencuri 50 juta data pengguna dan 7 juta mitra perusahaan jasa Uber. Data yang dicuri berupa info pribadi pengguna dan 600 ribu pelat nomor kendaraan mitra pengemudi Uber. *Chief Security Officer* (CSO) Uber mengatasi masalah tersebut dengan membayar uang tutup mulut senilai dengan Rp. 1,35 miliar kepada hacker (Jeko I. R, 2017).

Bukan hanya ancaman dari virus saja yang mengancam data dan informasi beserta aset infrastrukturnya. Bencana seperti gempa bumi di Myanmar yang merusak rumah dan Pagoda yang terjadi di beberapa kota seperti Shivezanthi, Taungpila, Kodaung, Tamagyaung, Chaungmagyi dan Tanyaung (Muslimah, S., 2016). Indonesia pun sering mengalami kerugian yang diakibatkan oleh bencana, seperti bencana gempa yang terjadi pada tahun 2006 yang merusak gedung seperti kampus STIE Kerja Sama yang rusak parah, Institute Seni Indonesia Yogyakarta mengalami kerusakan sangat parah dan beberapa swalayan di Yogyakarta (Martono, J., 2013) yang tentunya mengalami kerugian seperti hilangnya data dan informasi diakibatkan rusaknya aset-aset informasi tersebut.

Jika ancaman-ancaman dari informasi tersebut tidak segera ditanggulangi, maka akan menimbulkan risiko hilangnya data, informasi berserta infrastrukturnya pada aspek *confidentiality*, *integrity* dan *availability*. Akibatnya proses bisnis organisasi akan terhenti baik untuk sementara waktu bahkan dapat menyebabkan kehancuran sebuah organisasi.

Salah satu metode dalam mencegah dan meminimalisir ancaman keamanan informasi adalah metode *Maturity Level*. Metode tersebut berfungsi mengukur tingkat kematangan dari penerapan keamanan informasi pada organisasi. Beberapa penelitian yang menggunakan metode *Maturity Level* seperti perancangan audit keamanan informasi berdasarkan standar ISO 27001:2005 (Studi Kasus: PT. ADIRA DINAMIKA MULTI FINANCE) (Kristanto, dkk., 2014) yang meneliti perancangan audit dengan menggabungkan metode *Maturity Level* untuk mengukur kontrol keamanan yang diterapkan oleh organisasi. Kemudian pada penelitian *A Maturity Level Framework for Measurement of Information Security Performance* (Rosmiati, dkk., 2016) yang lebih menekankan metode *Maturity Level* sebagai metode analisis tingkat kematangan dari pengelolaan keamanan informasi yang telah diterapkan oleh organisasi, tingkat kematangan yang diharapkan oleh organisasi dan selisih (*Gap*) dari keduanya.

Metode *Maturity Level* adalah metode yang sangat tepat jika digunakan untuk mengukur seberapa matang organisasi dalam memanajemen keamanan informasi (Rosmiati, 2016). Dengan hasil dari analisis metode tersebut dapat memberikan

rekomendasi yang tepat sesuai dengan keadaan dari pengelolaan keamanan informasi yang telah diterapkan dan dapat pula untuk meningkatkan keamanan informasi sesuai dengan kebutuhan organisasi akan tetapi tergantung dengan data yang didapatkan ketika melaksanakan proses identifikasi data. Banyak metode yang digunakan agar data yang diberikan responden terjamin kevalidannya seperti metode observasi yang digabungkan dengan metode wawancara. Kelemahan metode observasi adalah tidak semua responden akan mau menunjukkan informasi misalkan informasi yang terkandung dalam aset informasi dikarenakan beberapa sebab seperti regulasi batasan daerah aman dan lain sebagainya.

Oleh sebab itu peneliti mencoba menggunakan metode Silogisme *AND* yang dimasukkan kedalam kuisioner wawancara. Memasukkan metode Silogisme *AND* kedalam Kuisioner bertujuan untuk mengetahui responden benar-benar valid dalam menjawab kuisioner tersebut. Keunggulan metode Silogisme *AND* adalah bahwa peneliti dapat menjamin kevalidan data yang diberikan oleh responden tanpa harus melaksanakan observasi, efisiensi waktu dikarenakan metode pengumpulan data yang dilaksanakan hanya satu kali, dikarenakan responden tidak tahu akan dimasukkannya metode Silogisme *AND* kedalam kuisioner, maka data akan tetap valid walaupun responden berbohong.

Dengan menggunakan metode Silogisme *AND* diharapkan data yang didapatkan adalah data yang valid atau sesuai dengan kondisi yang sebenarnya. Validitas data sangatlah penting dikarenakan jika data yang didapatkan adalah data yang valid, maka analisis metode *Maturity Level* lebih terjamin dan rekomendasi yang dihasilkan benar-benar dapat menangani ancaman dan risiko keamanan informasi pada organisasi tersebut.

Peneliti mengambil lokasi penelitian di Dinas Kependudukan dan Pencatatan Sipil Kota XYZ dikarenakan dinas tersebut adalah lembaga pemerintah yang menampung data masyarakat pada kota tersebut seperti identitas diri, data keluarga dan sampai data mutasi atau perpindahan. Oleh sebab itu lokasi yang diteliti adalah lokasi yang jika terkena gangguan keamanan informasi maka akan sangat fatal dampak yang didapatkan.

2. Kajian Literatur

2.1. Penelitian Terdahulu

Beberapa penelitian terdahulu yang dijadikan referensi seperti Kristanto (2014), Rosmiati (2016), meneliti tingkat kematangan keamanan infromasi pada suatu organisasi dengan menggunakan metode Capability Maturity Model (CMM) dan ISO 27001, metode tersebut mengidentifikasi ruang lingkup dalam menerapkan manajemen risiko. Peneliti tersebut menggabungkan metode audit dengan metode penilaian tingkat kedewasaan keamanan informasi untuk menilai tingkat kedewasaan dari keamanan informasi yang telah diterapkan organisasi berdasarkan standar ISO 27001 guna meminimalisir risiko dari informasi organisasi.

2.2. Keamanan Informasi

Keamanan informasi adalah hal yang sangat penting di abad modern ini, dikarenakan proses perpindahan data dan informasi dari bertuk fisik maupun tercetak menjadi bentuk digital dan terkomputerasi. Efek perubahan tersebut memberikan manfaat mudahnya informasi untuk diakses kapanpun ketika membutuhkan, terjaganya informasi dari kerusakan misal jika informasi tersebut dahulu berbentuk kertas, dan lebih mudah untuk digandakan.

Bagaikan pisau bermata dua, maka disamping mendapatkan manfaat informasi pun mendapatkan risiko dan ancaman, seperti halnya serangan malware WannaCry yang menyerang informasi pada seluruh dunia (Tribunnews.com, 2017), kemudian ancaman bencana alam yang tidak tentu terjadinya seperti banjir, gempa dan bencana lainnya yang menyebabkan rusaknya informasi beserta asetnya, begitupula dengan kejahatan spionase, hacking dan vanladism. Spionase bahkan pernah menyerang Presiden Indonesia pada selama 15 hari pada Agustus 2009 (LIPUTAN 6, 2013). Hacker juga mencuri 50 juta data pengguna dan 7 juta mitra perusahaan jasa Uber. Data yang dicuri berupa info pribadi pengguna dan 600 ribu pelat nomor kendaraan mitra pengemudi Uber. Chief Security Officer (CSO) Uber mengatasi masalah tersebut dengan membayar uang tutup mulut senilai dengan Rp. 1,35 miliar kepada hacker (LIPUTAN 6, 2017).

Keamanan informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis, memilimalisir risiko bisnis dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis (Sarno & Iffano, 2009).

Menurut Menteri Komunikasi dan Informatika, keamanan informasi adalah terjaganya kerahasiaan (confidentiality), keutuhan (integrity), dan ketersediaan (availability) informasi (Peraturan Menteri Komunikasi dan Informatika no 4 tahun 2016 pasal 1 ayat 6).

Keamanan informasi ditujukan untuk menjaga aspek kerahasiaan (Confidentiality), Keutuhan data atau informasi (Integrity) dan ketersediaan (Availability) dari informasi ketika diakses. Ketiga aspek yang sudah disebutkan sebelumnya biasanya disebut sebagai aspek keamanan informasi. Dibawah ini gambar yang menjelaskan aspek dari keamanan informasi menurut Sarno & Iffano (2009) :

Gambar 1. Aspek Keamanan Informasi (Sarno, 2009)

Untuk dapat meminimalisir dan memanajemen risiko pada keamanan informasi maka perlu diterapkan beberapa metode keamanan informasi, seperti *Risk Assessment* untuk menilai risiko pada aset informasi, *Maturity Level* untuk menilai tingkat keamanan informasi yang sudah diterapkan oleh organisasi dan menerapkan kebijakan keamanan informasi guna mengatur dan memanajemen keamanan informasi.

2.3. SNI ISO 27001:2013

SNI ISO 27001:2013 adalah sebuah Standar Nasional Indonesia untuk keamanan informasi yang mengadopsi standar internasional yaitu ISO 27001:2013. Standar tersebut adalah standar dokumen manajemen keamanan informasi yang didalamnya memberikan gambaran tentang apa yang seharusnya dilakukan oleh organisasi dalam usaha implementasi konsep keamanan informasi organisasi (Sarno, dkk., 2009). SNI ISO 27001:2013 telah merevisi SNI ISO 27001:2009 yang dulunya mengadopsi kepada ISO 27001:2005 terutama dari bagian penilaian risiko berbasis aset informasi menjadi penilaian risiko berbasiskan pemilik dari risiko.

2.4. Maturity Level

Maturity Level adalah salah satu alat pengukur dari kinerja suatu keamanan informasi (Sarno, 2009). Metode ini dapat mengevaluasi sendiri menjadi beberapa tingkat dari tingkat 0 yang artinya tidak ada penerapan kebijakan sedikitpun hingga tingkat 5 yang artinya penerapan kebijakan sudah teroptimalisasi. Model ini dibuat untuk mengetahui keberadaan dari sebuah masalah yang ada dan bagaimana menentukan prioritas peningkatan. Model ini dirancang sebagai profil dari proses keamanan informasi, sehingga perusahaan dapat mengambil keputusan penerapan keamanan informasi dari keadaan sekarang pada suatu organsiasi atau keadaan yang akan datang (Rosmiati, 2016). Berikut ini adalah tabel indeks *maturity level* dengan metode CMM (*Capability Maturity Model*) (Ruslam, 2013).

Tabel 1. *Indeks maturity level*

Indeks Kematangan	Tingkat Kematangan
0	0 *Non Existent*
0.2	1 *Initial/AdHoc*
0.4	2 *Repeatable but Intuitive*
0.6	3 *Defined Process*
0.8	4 *Managed and Measureable*
1	5 *Optimized*

Sumber: (Ruslam, 2013)

2.5. Conjungtion Rule (Aturan AND)

Sismoro (2005), menjelaskan bahwa pada aturan AND (Conjungtion Rule) akan bernilai benar (true) apabila proposisi penyusunannya bernilai benar (true). Apabila salah satu dari proposisi bernilai salah (false) atau semuanya bernilai salah (false) maka konjungsinya bernilai salah (false). Berikut ini adalah tabel dari conjungtion rule (Sismoro, 2005).

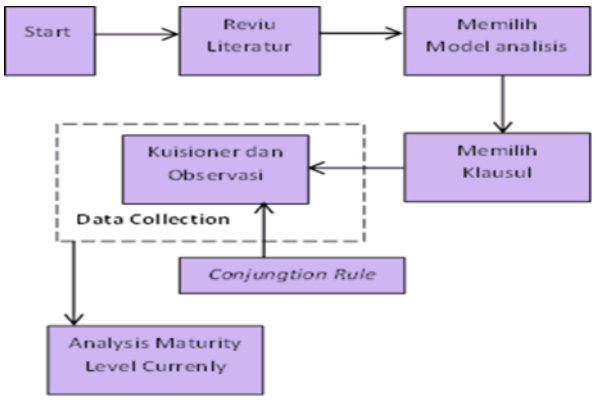
Tabel 2. *Conjungtion Rules*

P	Q	p ^ q
TRUE	TRUE	TRUE
TRUE	FALSE	FALSE
FALSE	TRUE	FALSE
FALSE	FALSE	FALSE

Sumber: (Sismoro, 2005)

3. Metode Penelitian

Metode penelitian yang dilaksanakan adalah metode wawancara kepada responden dengan metode *Maturity Level* dengan SNI ISO 27001:2013 sebagai acuan penilaian pengelolaan keamanan informasi yang didalam kuisioner tersebut dimasukkan metode Silogisme *AND* (Conjungtion Rule). Ruang lingkup penelitian adalah pada Sub Kontrol klausul A.7.2, A.7.3, A.9.1, A.9.2 dan A.9.3.



Gambar 2. Alur penelitian

Berikut ini adalah tabel aturan AND yang diterapkan pada kuisioner tiap klausul.

Tabel 3. *Kriteria silogisme pada sub kontrol A.7.2.1*

Sub Kontrol	Kuisioner Annex (QA)	Jawaban akan bernilai True
A.7.2.1	QA28	YA
A.7.2.1	QA59	TIDAK

Tabel 4. *Kriteria silogisme pada sub kontrol A.7.2.2*

Sub Kontrol	Kuisioner Annex (QA)	Jawaban akan bernilai True
A.7.2.2	QA29	YA
A.7.2.2	QA60	TIDAK

Tabel 5. *Kriteria silogisme pada sub kontrol A.7.3.1*

Sub Kontrol	Kuisioner Annex (QA)	Jawaban akan bernilai True
A.7.3.1	QA61	YA
A.7.3.1	QA62	TIDAK

Tabel 6. *Kriteria silogisme pada sub kontrol A.9.1.1*

Sub Kontrol	Kuisioner Annex (QA)	Jawaban akan bernilai *True*
A.9.1.1	QA32	YA
A.9.1.1	QA33	YA

Tabel 7. *Kriteria silogisme pada sub kontrol A.9.1.2*

Sub Kontrol	Kuisioner Annex (QA)	Jawaban akan bernilai *True*
A.9.1.2	QA63	YA
A.9.1.2	QA64	TIDAK

Tabel 8. *Kriteria silogisme pada sub kontrol A.9.2.1*

Sub Kontrol	Kuisioner Annex (QA)	Jawaban akan bernilai *True*
A.9.2.1	QA65	YA
A.9.2.1	QA66	TIDAK

Tabel 9. *Kriteria silogisme pada sub kontrol A.9.2.2*

Sub Kontrol	Kuisioner Annex (QA)	Jawaban akan bernilai *True*
A.9.2.2	QA67	YA
A.9.2.2	QA68	YA

Tabel 10. *Kriteria silogisme pada sub kontrol A.9.2.3*

Sub Kontrol	Kuisioner Annex (QA)	Jawaban akan bernilai *True*
A.9.2.3	QA69	YA
A.9.2.3	QA70	TIDAK

Tabel 11. *Kriteria silogisme pada sub kontrol A.9.2.4*

Sub Kontrol	Kuisioner Annex (QA)	Jawaban akan bernilai *True*
A.9.2.4	QA71	YA
A.9.2.4	QA34	YA

Tabel 12. *Kriteria silogisme pada sub kontrol A.9.2.5*

Sub Kontrol	Kuisioner Annex (QA)	Jawaban akan bernilai *True*
A.9.2.5	QA35	YA
A.9.2.5	QA72	TIDAK

Tabel 13. *Kriteria silogisme pada sub kontrol A.9.3.1*

Sub Kontrol	Kuisioner Annex (QA)	Jawaban akan bernilai *True*
A.9.3.1	QA73	YA
A.9.3.1	QA74	TIDAK

Pada tabel tersebut terdapat kolom jawaban akan bernilai *true* maksudnya adalah kriteria bernilai true adalah pada setiap kolom dalam tabel tersebut. Semisal jawaban yang diberikan responden adalah TIDAK seperti pada kuisioner QA74 sub kontrol A.9.31 akan menghasilkan nilai *true*.

4. Hasil dan Pembahasan

Setelah merancang, mengidentifikasi dan mengumpulkan data yang dibutuhkan, langkah selanjutnya adalah menentukan hasil dan pembahasan yaitu menganalisis data yang sudah dikumpulkan sebelumnya. Hasil dan pembahasan ini lebih fokus terhadap analisis *maturity level* yang digabungkan dengan metode Silogisme *AND* (Conjungtion Rule). Setelah nilai didapatkan, maka nilai dari setiap sub kontrol digabungkan kedalam setiap klausul SNI ISO 27001:2013. Berikut ini tabel nilai *maturity level* untuk setiap kontrol.

Tabel 14. *Nilai maturity level kontrol A.7.2*

Sub Kontrol	Nilai
A.7.2.1	0
A.7.2.2	0
A.7.2.3	1
Hasil	**0,33**

Tabel 15. *Nilai maturity level kontrol A.7.3*

Sub Kontrol	Nilai
A.7.3.1	1
Hasil	**1**

Tabel 16. *Nilai maturity level kontrol A.9.1*

Sub Kontrol	Nilai
A.9.1.1	1
A.9.1.2	1
Hasil	**1**

Tabel 17. *Nilai maturity level kontrol A.9.2*

Sub Kontrol	Nilai
A.9.2.1	1
A.9.2.2	1
A.9.2.3	1
A.9.2.4	0
A.9.2.5	0
Hasil	**0,6**

Tabel 18. *Nilai maturity level kontrol A.9.3*

Sub Kontrol	Nilai
A.9.3.1	1
Hasil	**1**

Dari hasil pengelompokan hasil nilai sub kontrol kedalam tiap kontrol maka langkah selanjutnya menentukan nilai *maturity level* dalam tiap klausul. Nilai *maturity level* dalam setiap klausul yang akan mendefinisikan apakah tingkat kematangan pengelolaan informasi sudah baik apakah masih perlu ditingkatkan. Berikut ini tabel analisi *maturity level* dalam setiap klausul SNI ISO 27001:2013.

Tabel 19. *Analisis maturity level pada klausul A.7*

Kotrol	Nilai
A.7.2	0,33
A.7.3	1
Hasil	**0,67**

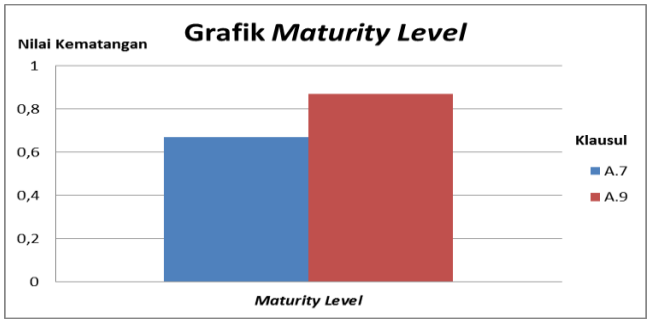
Tabel 20. *Analisis maturity level pada klausul A.8*

Kotrol	Nilai
A.9.1	1
A.9.2	0,6
A.9.3	1
Hasil	**0,87**

Langkah selanjutnya adalah menentukan *maturity level* dari hasil analisis maturity level pada setiap klausul. Berikut ini adalah tabel dan grafik *maturity level* dari pengelolaan keamanan informasi pada setiap klausul SNI ISO 27001:2013 yang dianalisis.

Tabel 21. *Maturity level dari pengelolaan keamanan informasi*

Klausul	Nilai *Maturity Level*	*Maturity Level*
A.7	**0,67**	**3**
A.9	**0,87**	**4**



Gambar 3. *Grafik maturity level pengelolaan informasi*

5. Kesimpulan

Kesimpulan dari hasil penelitian menggabungkan metode Silogisme *AND* yaitu dengan menggunakan conjungtion rule dapat diterapkan sebagai metode untuk validitas jawaban yang diberikan responden. Metode Silogisme *AND* memberikan kontribusi dalam pemberian rekomendasi kontrol keamanan yang harus ditingkatkan/dikelola dikarenakan semakin valid jawaban yang diberikan oleh responden dalam analisis *maturity level* maka semakin teridentifikasi kelemahan pengelolaan keamanan informasi pada organisasi dan dengan hal tersebut maka akan memberikan rekomendasi penanganan yang lebih tepat dan sesuai dengan kebutuhan organisasi.

Saran untuk penelitian selanjutnya adalah untuk mengembangkan metode Silogisme lain selain conjungtion rule yang dikolaborasikan kedalam metode Analisis *Maturity level* untuk validitas jawaban dari responden.

Daftar Pustaka

Jurnal:

Kristanto, T., Rachman, A. & Fakhrur Rozi, N., (2014). Perancangan Audit Keamanan Informasi berdasarkan Standar ISO 27001:2005 (Studi Kasus: PT Adira Dinamika Multi Finance), SESINDO

Rosmiati, Riadi, I., (2016). Analisis Keamanan Informasi Berdasarkan Kebutuhan Teknikal dan Operasional Mengkombinasikan Standar ISO 27001:2005 dengan *Maturity level* (Studi Kasus Kantor Biro Teknologi Informasi PT. XYZ), Seminar Nasional Teknologi Informasi dan Multimedia, STMIK AMIKOM Yogyakarta, Yogyakarta

Rosmiati, Riadi I. & Prayudi Y., (2016). *A Maturity Level Framework for Measurement of Information Security Performance*, International Journal of Computer Aplications

(0975-8887), Volume 141 No. 8

Buku:

BSN, (2016). Standar Nasional Indonesia (SNI) ISO 27001:2013, BSN, Jakarta

Sarno, R., (2009). Audit Sistem & Teknologi Informasi, ITS Press, Surabaya

Sarno, R. & Iffano, I., (2009). Sistem Manajemen Keamanan Informasi, ITS Press, Surabaya

Sismoro, (2005). Pengantar Logika Informatika, Algoritma dan Pemrograman Komputer, Andi Publisher, Yogyakarta

Skripsi/tesis/disertasi:

Ruslam, R., Z., (2013). Audit Kepatuhan Keamanan Informasi dengan Menggunakan *Framework* ISO 27001/ISMS pada PT. XYZ, Tesis, Fakultas Ilmu Komputer Magister Teknologi Informasi Universitas Indonesia, Jakarta

Internet:

ANTARA, (2017). *Virus Komputer Ransomware Kembali Menyerang Sejumlah Negara*, 2017.Website:https://tekno.kompas.com/read/2017/06/28/06153547/virus.komputer.ransomware.kembali.menyerang.sejumlah.negara, diakses tanggal 07 Mei 2018

Jeko I. R, (2017). *Kronologi Puluhan Juta Data Pengguna Uber Dicuri*, 2017. Website: http://tekno.liputan6.com/read/3171282/kronologi-puluhan-juta-data-pengguna-uber-dicuri, diakses tanggal 07 Mei 2018

Muslimah, S., (2016). *Ini Analisis BMKG Soal Gempa 6,8 SR yang Guncang Myanmar*, 2016. Website: https://news.detik.com/berita/3283139/ini-analisis-bmkg-soal-gempa-bumi-68-sr-yang-guncang-myanmar, diakses tanggal 07 Mei 2018

Martono, J., (2013). *Mengenang Gempa Tektonik 2006 di Yogyakarta dan Sekitarnya (1)*, 2013. Website: https://www.kompasiana.com/jk.martono/mengenang-gempa-tektonik-2006-di-yogyakarta-dan-sekitarnya-1_5520a164a33311764646d137, diakses tanggal 07 Mei 2018

Pratiwi, D., (2017). *Virus WannaCry Menyerang 17 Perusahaan di Korea Selatan*, 2017. Website: http://www.tribunnews.com/techno/2017/05/18/virus-wannacry-menyerang-17-perusahaan-di-korea-selatan, diakses tanggal 07 Mei 2018