ANALISIS KEAMANAN INFORMASI BERDASARKAN KEBUTUHAN TEKNIKAL DAN OPERASIONAL MENGKOMBINASIKAN STANDAR ISO 27001:2005 DENGAN *MATURITY LEVEL* (Studi Kasus Kantor Biro Teknologi Informasi PT. XYZ)

Rosmiati[1)], Imam Riadi[2)]

[1),] Magister Teknik Informatika Universitas Islam Indonesia Yogyakarta
Jl Kaliurang KM 14.5, Sleman, Yogyakarta 55584
[2)] Teknologi Industri Universitas Ahmad Dahlan
Jl Jalan Prof. Dr. Soepomo, S.H. Janturan Yogyakarta 55164
Email : rosedipanegara@gmail.com[1)], imam.riadi@is.uad.ac.id[2)],

Abstrak

Informasi merupakan salah satu aset perusahaan yang sangat penting. Dengan perkembangan teknologi informasi yang sangat pesat, kemungkinan terjadinya gangguan keamanan informasi semakin meningkat. Penerapan keamanan informasi dimaksudkan untuk mengatasi segala masalah dan kendala baik secara teknis maupun secara non-teknis. Penelitian ini dilakukan untuk mengetahui tingkat keamanan informasi pada PT. XYZ untuk memberikan rekomendasi perbaikan dan peningkatan dalam pengelolaan keamanan informasi pada perusahaan.

ISO 27001 berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI). Sumber data yang digunakan dalam penelitian ini adalah kuisioner. Responden dalam penelitian ini adalah semua karyawan/pegawai yang berada dalam kantor Biro Teknologi Informasi PT. XYZ sebanyak 14 orang.

Hasil penelitian menunjukkan maturity level keamanan informasi pada Kantor Biro Teknologi Informasi PT. XYZ berada pada level 2. Nilai kesenjangan antara nilai maturity level saat ini dan nilai maturity level yang diharapkan adalah 0.79. Rekomendasi perbaikan yang diberikan membutuhkan pemahaman tentang perusahaan dan juga dibutuhkan koordinasi dengan pihak internal perusahaan.

Kata kunci: *Informasi, Keamanan Informasi, ISO 27001, Maturity Level, Nilai Kesenjangan.*

1. Pendahuluan

Sebagian besar proses pengelolaan adminsistrasi di perusahaan telah menggunakan sistem elektronik yang menyimpan begitu besar informasi secara digital dan menggunakan jalur atau jaringan teknologi informasi dalam berkomunikasi. Dengan kata lain, kegiatan bisnis, administrasi, dan publik bergantung pada sistem informasi apa yang digunakannya. Seperti yang dilakukan oleh manajemen PT. XYZ yang tidak dapat mengabaikan sistem informasi karena sistem informasi secara signifikan telah mempengaruhi dan mengubah cara bisnis yang sedang dikelola dan dipantau saat ini [1]. Oleh karena itu, suatu hal yang penting untuk memahami dan mengimplementasikan keamanan informasi pada sistem informasi yang digunakan, baik untuk kalangan organisasi bisnis/swasta maupun instansi pemerintahan. Penerapan keamanan informasi dimaksudkan untuk mengatasi segala masalah dan kendala baik secara teknis maupun non-teknis seperti faktor ketersediaan (availability), kerahasiaan (confidentiality), dan kesatuan (integrity). Untuk itu perusahaan harus menerapkan kebijakan yang tepat untuk melindungi aset informasi yang dimiliki. Salah satu kebijakan yang dapat diambil oleh perusahaan untuk mengatasi gangguan keamanan informasi adalah dengan menerapkan Sistem Manajemem Keamanan Informasi (SMKI).

Menurut Bundesamt fur Sicherheit in der information stechnik (2008) “BSI-Standard 100-1 : Information Security Management System (ISMS)” bahwa SMKI (Sistem Manajemen Keamanan Informasi) menentukan instrumen dan metode yang digunakan harus jelas dalam pengelolaan (merencanakan, mengadopsi, menerapkan, mengawasi, dan meningkatkan) tugas dan kegiatan yang ditujukan untuk mencapai keamanan informasi[2]. Keamanan informasi secara tidak langsung menjadi salah satu perhatian bagi perusahaan jika ingin melanjutkan bisnisnya. Oleh karena itu, perlu adanya standarisasi yang diterapkan atau diimplementasikan dalam perusahaan sebagai panduan yang memberikan arahan dalam menjaga aset penting seperti informasi yang dianggap sensitive bagi perusahaan tersebut.

Dalam analisis teknologi informasi terdapat beberapa framework atau kerangka kerja yang mengacu kepada referensi tata kelola teknologi informasi internasional yang telah diterima secara luas dan teruji implementasinya yaitu ISO 27001, COBIT dan ITIL, yang dapat diimplemetasikan sesuai dengan kondisi perusahaan yang berbeda-beda. Untuk membantu organisasi dalam menganalisa sistem keamanan informasi, standar yang digunakan adalah standar ISO 27001. Hal yang dijadikan pertimbangan mengapa standar ISO/IEC 27001 dipilih karena di PT. XYZ

membuat Standar Operasional Prosedur (SOP) dengan menggunakan standar ISO 27001 tetapi belum dilakukan tinjauan ulang / update, sehingga masih terjadi gangguan keamanan pada pengelolaan keamanan informasi.

Sehubungan dengan alasan tersebut, diperlukan adanya analisis tingkat kematangan keamanan informasi terhadap pengelolaan keamanan informasi pada PT. XYZ untuk mengetahui penyebab permasalahan keamanan informasi yang selama ini terjadi. Tujuan dari penelitian ini adalah melakukan pengukuran tingkat kematangan (*maturity level*) keamanan informasi pada PT. XYZ menggunakan ISO 27001.

1.1 Keamanan Informasi

Keamanan informasi merupakan upaya untuk melindungi aset informasi yang dimiliki. Upaya perlindungan tersebut dimaksudkan untuk memastikan keberlanjutan bisnis, meminimalkan risiko yang mungkin terjadi dan memaksimalkan keuntungan yang didapat dari investasi dan kesempatan bisnis [3].
Keamanan bisa dicapai dengan beberapa cara atau strategi yang biasa dilakukan secara stimultan atau dilakukan dalam kombinasi satu dengan yang lainnya. Strategi dari keamanan informasi masing-masing memiliki fokus dan dibangun tujuan tertentu sesuai kebutuhan [4]. Contoh keamanan informasi antara lain :

1. *Physical security*
2. *Personal security*
3. *Operation security*
4. *Communication security*
5. *Network security*

Aspek-aspek keamanan informasi dalam suatu organisasi dapat dilihat pada Gambar 1[4]:

Gambar 1. *Aspek Keamanan Infromasi*

1. Confidentiality adalah keamanan informasi seharusnya menjamin bahwa hanya mereka yang memiliki hak yang boleh mengakses informasi tertentu.
2. Integrity adalah keamanan informasi seharusnya menjamin kelengkapan informasi dan menjaga dari korupsi, kerusakan atau ancaman lain yang menyebabkan berubahnya informasi dari aslinya.
3. Availability adalah keamanan informasi seharusnya menjamin pengguna dapat mengakses informasi kapanpun tanpa adanya gangguan dan tidak dalam format yang tidak bisa digunakan

1.2 ISO 27001

ISO/IEC 27001:2005 merupakan standard keamanan informasi yang diterbitkan *International Organization for Standarization* dan *International Electrotecnical Comission* pada bulan Oktober 2005 untuk menggantikan standard BS7799-2. Standard ini berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI). Standar ini bersifat independen terhadap produk teknologi informasi, mensyaratkan penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk menjamin agar kontrol-kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi pihak yang berkepentingan [5].

Latar belakang disusunnya standar ISO 27001 untuk manajemen keamanan informasi adalah karena diperlukannya suatu cara bagaimana data atau informasi tersebut dikelola, dipelihara dan diekspos[7]. Awalnya ISO 27001 adalah standar internasional yang menyediakan petunjuk dan kontrol untuk mengatur keamanan informasi.

Stuktur organisasi ISO 27001 dibagi menjadi dalam dua bagian besar yaitu [4] :

1. Klausul : *Mandatory Process*

   Klausul adalah persyaratan yang harus dipenuhi jika organisasi menerapkan SMKI dengan menggunakan standar ISO 27001

2. Annex A : *Security Control*

   Annex A adalah dokumen referensi yang disediakan dan dapat dijadikan rujukan untuk menentukan kontrol keamanan apa (*security control*) yang perlu diimplementasikan dalam SMKI, yang terdiri dari 11 klausul kontrol keamanan, 39 kontrol objektif dan 133 kontrol.

ISO 27001 mendefinisikan 133 buah kontrol keamanan yang terstruktur dan dikelompokkan menjadi 11 klausul untuk memudahkan dalam mengidentifikasi hal-hal yang dibutuhkan untuk mengamankan aset informasi perusahaan. Klausul yang terdapat dalam standar ISO 27001 dapat dilihat pada Tabel 1[4].

Tabel 1 *Jumlah Klausul Kontrol Keamanan*

Klausul	Jumlah	
	Objektif Kontrol	Kontrol
5 (Kebijakan keamanan)	1	2
6 (Organisasi Keamanan Informasi)	2	11
7 (Manajemen Aset)	2	5
8 Keamanan SDM	3	9

Klausul	Jumlah	
	Objektif Kontrol	Kontrol
9 (Keamanan Fisik dan Lingkungan)	2	13
10 (Manajemen Komunikasi dan Operasi)	10	31
11 (Persyaratan Bisnis untuk Akses Kontrol)	7	25
12 (Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan)	6	16
13 (Manajemen Insiden Keamanan Informasi)	2	5
14 (Manajemen Kelangsungan Bisnis)	1	5
15 (Kepatutan)	3	10
Jumlah = 11	39	133

Klausul klausul tersebut dapat dikelompokkan menjadi tiga kelompok kebutuhan kontrol keamanan yaitu manajemen/organisasi, teknikal dan operasional seperti terlihat pada Tabel 2[4].

Tabel 2. *Kebutuhan Kontrol Keamanan*

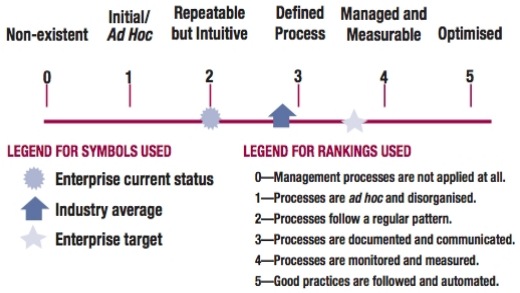
Kategori Kebutuhan	Klausul
Manajemen	5
	6
	7
	15
Teknikal	8
	9
	11
	12
Operasional	10
	13
	14

Pengelompokan kebutuhan kontrol keamanan sangat penting, untuk memudahlan perushaan memilih atau menentukan kontrol keamanan yang dibutuhkan baik dalam hubungannya dengan kebutuhan Kontrol keamanan secara manajemen, teknikal dan operasional maupun juga jika diperlukan kebutuhan kontrol keamanan dalam penjagaan keamanan informasi yaitu aspek keamanan informasi.

1.3 Maturity Level

Salah satu alat pengukuran dari kinerja suatu keamanan informasi adalah model kematangan (*maturity level*)[5]. Model kematangan untuk pengelolaan dan pengendalian pada proses sistem informasi didasarkan pada metode evaluasi organisasi sehingga dapat mengevaluasi sendiri dari level 0 (tidak ada) hingga level 5 (optimis). Model kematangan dimaksudkan untuk mengetahui keberadaan persoalan yang ada dan bagaimana menentukan prioritas peningkatan. Model kematangan dirancang sebagai profil proses keamanan infromasi, sehingga perusahaan akan dapat mengenali sebagai deskripsi kemungkinan keadaan sekarang dan mendatang. Penggunaan model kematangan yang dikembangkan untuk setiap 39 objektif kontrol pada ISO 27001 memungkinkan manajemen perusahaan dapat mengidentifikasi [8] : (1) Kondisi perusahaan sekarang. (2) Kondisi sekarang dari industri untuk perbandingan. (3) Kondisi yang diinginkan perusahaan. (4) Pertumbuhan yang diinginkan.

Gambar 2 menunjukkan urutan tingkat kematangan keamanan informasi dalam perusahaan[8].



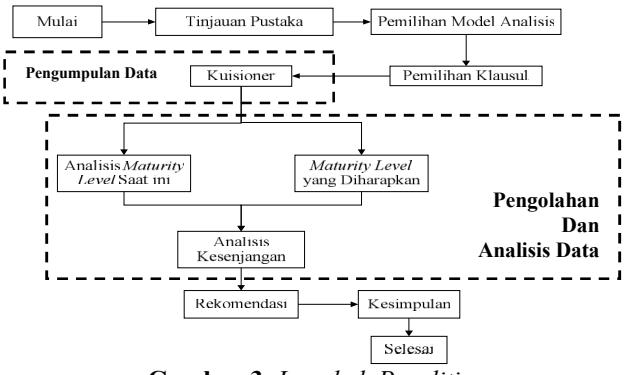
Gambar 2. *Urutan Tingkat Kematangan*

Jika dikelompokkan berdasarkan nilai level keamanan maka dirinci seperti Tabel 3[4].

Tabel 3. *Level Kematangan Informasi*

Indeks Kematangan	Level Kematangan
0 - 0.49	0 *Non Existent*
0.50 – 1.49	1 *Initial / AdHoc*
1.50 – 2.49	2 *Repeatable But Intutitive*
2.50 – 3.49	3 *Defined Process*
3.50 – 4.49	4 *Managed and Measureable*
4.50 – 5.00	5 *Optimized*

Dalam penelitian ini metode yang digunakan adalah metode penelitian kuantitatif, data diperoleh dari hasil penyebaran kuisioner yang diberikan kepada responden. Responden dalam penelitian ini adalah seluruh karyawan yang berada dalam kantor Biro Teknologi Informasi PT. XYZ yang berjumlah 14 orang. Pengolahan dan analisis hasil penelitian dilakukan dengan menggunakan MS Excel 2007. Urutan langkah-langkah penelitian dapat dilihat pada Gambar 3.



Gambar 3. *Langkah Penelitian*

2. Pembahasan

2.1 Hasil Perhitungan Data

Stukrtur ISO 27001 yang digunakan dalam penelitian ini adalah bagian Annex A (*Security Control*) yang terdiri dari 39 objektif kontrol dan 133 kontrol namun tidak melibatkan klausul utama yang ada di dalam ISO 27001. Hal ini dilakukan karena agar hasil penelitian lebih mendetail seperti dapat mengetahui kontrol-kontrol kemanan yang lemah. Dengan mengetahui kontrol-kontrol yang lemah, maka manajemen perusahaan bisa mengambil tindakan untuk memperbaiki kontrol-kontrol yang membutuhkan penanganan. Perusahaan juga bisa menjaga konsistensi dalam menjaga keamanan informasi.

Nilai *maturity* diperoleh dari hasil rata-rata jawaban responden terhadap masing-masing klausul yang terdapat pada standar ISO 27001, sedangkan nilai kematangan yang diharapkan (*Expected Maturity)* diperoleh berdasarkan nilai rata-rata seluruh atribut nilai kematangan untuk proses-proses yang dinilai[6]. Setelah semua hasil kuisioner dimasukkan kedalam tabel, kemudian dihitung tingkat kematangan tiap proses dalam masing-masing klausul untuk tiap responden. Hasil *maturity level* tiap klausul dari 14 responden kemudian dicari rata-ratanya, dan rata-rata tersebut akan menjadi nilai *maturity level* atau tingkat kematangan keamanan informasi. Tabel 4 menunjukkan hasil perhitungan kuisioner untuk mendapatkan tingkat kematangan keamanan informasi.

Tabel 4. *Hasil Perhitungan Tingkat Kematangan Keamanan Informasi*

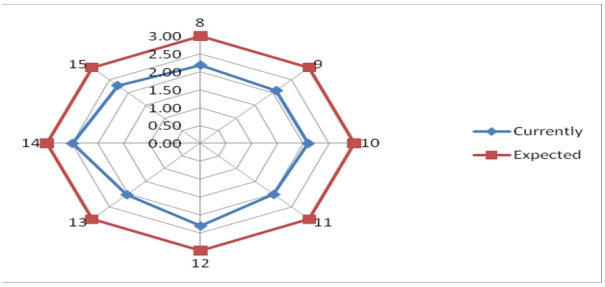
Klausul	Proses	Nilai	Level
8	Keamanan SDM	2.19	2
9	Keamanan Fisik dan Lingkungan	2.09	2
10	Manajemen Komunikasi dan Operasi	2.10	2
11	Persyaratan Bisnis untuk Akses Kontrol	2.02	2
12	Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan	2.31	2
13	Manajemen Insiden Keamanan Informasi	2.03	2
14	Manajemen Kelangsungan Bisnis	2.50	3
	Rata-rata	2.18	2

Berdasarkan hasil *maturity level* dari hasil penyebaran kuisioner, kemudian dihitung nilai kesenjangan antara *maturity level* saat ini dengan *maturiry level* yang diharapkan. Tabel 5 menunjukkan nilai kesenjangan keamanan informasi di Kantor Biro Teknologi Informasi PT. XYZ.

Tabel 5. *Nilai Kesenjangan Keamanan Informasi*

Klausul	Tingkat Kematangan		Nilai Kesenjangan
	Saat ini	Yang diharapkan	
8	2.19	3.00	0.81
9	2.09	3.00	0.91
10	2.10	3.00	0.90
11	2.02	3.00	0.98
12	2.31	3.00	0.69
13	2.03	3.00	0.97
14	2.50	3.00	0.50

Nilai kesenjangan antara nilai *maturiry level* saat ini dengan nilai *maturiry level* yang diharapkan dapat dilihat pada Gambar 3.



Gambar 3. *Nilai Perbandingan maturiry level saat ini dan yang diharapkan*

2.2 Analisa Hasil Penelitian

Berdasarkan hasil penelitian, maka didapatkan hasil analisa keamanan dengan mengkombinasikan ISO 27001 dengan *maturity level* seperti dibawah ini:

1. Klausul 8 Keamanan SDM

   Berdasarkan hasil perhitungan *maturiry level*, nilai yang diperoleh pada klausul 8 tentang keamanan SDM berada pada tingkat *Repeatable But Intutitive* pada posisi nilai 2.19 yang berarti saat ini keamanan informasi pada Kantor Biro Teknologi Informasi PT. XYZ harus dikembangkan kedalam tahapan yang lebih baik. Tidak adanya prosedur mengenai pengelolaan hak akses pengguna sehingga siapa saja yang bisa masuk kedalam lingkungan Kantor Biro Teknologi Informasi akan dengan mudah mengelola hak akses pengguna. Oleh karena itu dibutuhkan sebuah tim/perorangan yang bertugas dan bertanggung jawab mengatur dan mengelola hak akses user, kemudian pengelolaan tersebut berdasarkan pada prosedur dan kebijakan yang dikeluarkan perusahaan. Selain itu diperlukan Sumber Daya Manusia (SDM) yang penuh tanggung jawab dan profesional.

2. Klausul 9 Keamanan Fisik dan Lingkungan

   Berdasarkan hasil perhitungan *maturiry level*, nilai yang diperoleh pada klausul 9 tentang Keamanan Fisik dan Lingkungan berada pada tingkat *Repeatable But Intutitive* pada posisi nilai 2.09 yang berarti saat ini keamanan informasi pada Kantor Biro

Teknologi Informasi PT. XYZ harus dikembangkan kedalam tahapan yang lebih baik. Akses terhadap lokasi fisik yang menyimpan pusat informasi harus dibatasi agar terhindar dari kemungkinan terjadinya pengrusakan yang dilakukan oleh pihak yang tidak bertanggung jawab. Pada saat ini lokasi penyimpanan server jauh dari keramaian dan akses orang banyak, ruangan server dilengkapi AC, kamera CCTV, kunci dan pengamanan dari kebakaran. Terdapat pula larangan akses fisik terhadap server yang berupa larangan msuk selain orang yang berwenang.

3. Klausul 10 Manajemen Komunikasi dan Operasi

   Berdasarkan hasil perhitungan *maturiry level*, nilai yang diperoleh pada klausul 10 tentang Manajemen Komunikasi dan Operasi berada pada tingkat *Repeatable But Intutitive* pada posisi nilai 2.10 yang berarti saat ini keamanan informasi pada Kantor Biro Teknologi Informasi PT. XYZ harus dikembangkan kedalam tahapan yang lebih baik. Saat ini Kantor Biro Teknologi Informasi PT. XYZ telah memiliki SOP sebagain landasan dalam pengoperasian sistem informasi, *back-up* dan pemeliharaan peralatan. Namun belum ada kontrol pencegahan, deteksi dan respon terhadap *software* yang berbahaya.

4. Klausul 11 Persyaratan Bisnis untuk Akses Kontrol

   Berdasarkan hasil perhitungan *maturiry level*, nilai yang diperoleh pada klausul 11 tentang Manajemen Komunikasi dan Operasi berada pada tingkat *Repeatable But Intutitive* pada posisi nilai 2.02 yang berarti saat ini keamanan informasi pada Kantor Biro Teknologi Informasi PT. XYZ harus dikembangkan kedalam tahapan yang lebih baik. Tidak ada pembatasan dan pengaturan terhadap alokasi pengguna hak akses istimewa dan khusus. Tidak ada kebijakan dalam perubahan *password* secara berkala. Kerahasiaan *password* kurang baik karena data yang tersimpan kedalam basis data bukan hasil enkripsi.

5. Klausul 12 Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan

   Berdasarkan hasil perhitungan *maturiry level*, nilai yang diperoleh pada klausul 12 tentang Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan berada pada tingkat *Repeatable But Intutitive* pada posisi nilai 2.31 yang berarti saat ini keamanan informasi pada Kantor Biro Teknologi Informasi PT. XYZ harus dikembangkan kedalam tahapan yang lebih baik. Sistem informasi merupakan sistem yang interaktif karena setiap validasi, sistem akan mengeuarkan pesan yang terkait dengan kegiatan dengan kegiatan yang dilakukan oelh pengguna. Namun belum adanya kebijakan tentang penggunaan kontrol kriptografi untuk proteksi informasi yang seharusnya dikembangkan dan diimplemtasikan. Tidak adanya pembatasan terhadap akses ke *source* program.

6. Klausul 13 Manajemen Insiden Keamanan Informasi

   Berdasarkan hasil perhitungan *maturiry level*, nilai yang diperoleh pada klausul 13 tentang Manajemen insiden keamana informasi berada pada tingkat *Repeatable But Intutitive* pada posisi nilai 2.03 yang berarti saat ini keamanan informasi pada Kantor Biro Teknologi Informasi PT. XYZ harus dikembangkan kedalam tahapan yang lebih baik. Tidak ada prosedur atau kebijakan tentang pelaporan insiden, pengguna melakukan sesuai inisiatif sendiri. Tidak bekerjanya sistem yang dapat melakukan pemantauan terhadap ancaman keamanan informasi mengakibatkan seringnya pengrusakan data dilakukan oleh pihak yang tidak bertanggung jawab.

7. Klausul 14 Manajemen Kelangsungan Bisnis

   Berdasarkan hasil perhitungan *maturiry level*, nilai yang diperoleh pada klausul 14 tentang Manajemen insiden keamana informasi berada pada tingkat *Defined Process* pada posisi nilai 2.50 yang berarti saat ini keamanan informasi pada Kantor Biro Teknologi Informasi PT. XYZ saat ini prosedur distandarisasi dan didokumentasikan kemudian dikomunikasikan melalui pelatihan. Adanya kerangka kerja yang bisa digunakan untuk merencanakan keberlangsungan bisnis dan adanya kegiatan percobaan atas perencanaan yang telah disusun. Selain itu sudah ada prosedur pengelolaan dalam pengembangan dan mempertahankan kelangsungan bisnis.

Dari hasil perhitungan tingkat kematangan keamanan informasi, dimana tingkat kematangan yang menjadi acuan dalam penelitian ini adalah pada level 3 (*Defined Process*). Berdasarkan hasil perhitungan yang telah dilakukan maka dapat diperoleh bahwa tingkat kematangan keamanan informasi pada PT. XYZ adala rata-rata berada pada level 2. Berarti bahwa saat ini keamanan informasi pada PT. XYZ harus diperbaiki dan dikembangkan ke tahap yang lebih baik karena masih berada dibawah level 3.

3. Kesimpulan

Berdasarkan hasil penelitian dan pengelolaan data yang berkaitan dengan keamanan informasi dengan menggunakan kombinasi ISO 27001 dengan *maturity level* pada PT. XYZ dapat ditarik kesimpulan sebagai berikut :

1. Tingkat kematangan keamanan informasi pada kantor Biro Teknologi Informasi rata-rata masih berada di tingkat kedua (*Repeatable But Intituive*) yaitu klausul Keamanan SDM, Keamanan Fisik dan Lingkungan, Manajemen Komunikasi dan Operasi, Persyaratan Bisnis untuk Akses Kontrol, Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan, Manajemen Insiden Keamanan Informasi berada pada tingkat kedua (*Repeatable But Intituive*). Sedangkan klausul Manajemen Kelangsungan Bisnis berada pada Tingkat ketiga (*Defined Process*).
2. Penerapan standarisasi keamanan informasi pada PT. XYZ berdasarkan kebutuhan teknikal dan

operasional menggunakan ISO 27001 masih belum siap karena 7 klausul yang ditetapkan hanya 1 klausul saja yang memenuhi standar yaitu klausul Manajemen Kelangsungan Bisnis.

3. Peranan standar ISO 27001 dalam menjaga keamanan informasi yang tersimpan adalah sebagai acuan dalam melakukan kontrol keamanan informasi berdasarkan resiko, peraturan, hukum dan undang-undang serta prinsip, tujuan dan kebutuhan informasi pada informasi.

Daftar Pustaka

[1] J.E. Bunton & N.A. Bagnaroff. *Information Technologi Auditing*. Wiley. 2004.

[2] Bundesamt Fur Sicherheit in der Informatmationstechnik (BSI), *BSI Standard 100-1 Information Security Mangement System (ISMS)*. Bonn. 2008.

[3] M. Utomo, A. Holil, I. Affandi, "Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 pada Kantor Pelayanan Perbendaharaan Surabaya I", *Jurnal Teknik ITS Vol. 1, no.1*, ISSN:2301-9271, pp. 288-293, September 2012.

[4] Sarno, Riyanarto, *"Sistem Manajemen Keamanan Informasi berbasis ISO 27001"*. Surabaya: ITS Press, 2009.

[5] Standar Nasional Indonesia, Teknologi Informasi – Teknik Kemanan – Sistem Manajemen Keamanan Informasi – Persyaratan (ISO/IEC 27001:2005*)*.

[6] F. Ermana, H. Tanuwijaya, I.A. Mastan, *"Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27001 pada PT. BPR Jatim*. STIKOM Surabaya. 2012

[7] A. Supriyatna, "Analisis Tingkat Kematangan Keamanan Sistem Informasi Akademik dengan Mengkombinasikan Standar BS-7799 dengan SSE-CMM", *Prosiding Seminar Nasional Aplikasi Sains & Tehnologi (SNAST)*, ISSN: 1979-911X, pp. 181-188, November 2014.

[8] IT Governance Intitute. "*Framework Control Objectives Management Guidelines Maturity Models*", USA. 2007.

Biodata Penulis

Rosmiati, memperoleh gelar Sarjana Komputer (S.Kom), Jurusan Sistem Informasi STMIK DIPANEGARA Makassar, lulus tahun 2012. Saat ini sedang menyelesaikan masa studi Magister di Magister Teknik Informatika di Universitas Islam Indonesia, Yogyakarta

Imam Riadi, memperoleh gelar Doktor (Dr.), Jurusan Ilmu Komputer Universitas Gajah Mada Yogyakarta, lulus tahun 2014. Saat ini menjadi Dosen di Universitas Ahmad Dahlan (UAD) Yogyakarta.