ISSN: 2087-1716
ILKOM Jurnal Ilmiah Volume 8 Nomor 3 (Desember 2016)

ANALISIS KEAMANAN JARINGANPADA BALAI KARANTINA PERTANIAN KELAS II GORONTALO

Rachmad Arissaputra Ipango[1], Bambang Soedijono W[2], Roy Rudolf Huizen[3]
rexxar436@gmail.com[1], bambang.s@amikom.ac.id[2], royrudolf.usm@gmail.com[3]
[1,2,3] Teknik Informatika STMIK AMIKOM Yogyakarta

Abstrak

Penelitian ini bertujuan untuk mengukur tingkat keamanan pada Balai Karantina Pertanian Kelas II Gorontalo dengan menggunakan *framework* ISO 27001 sehingga dapat diketahui sejauh mana proses pengamanannya dan kondisi dari keamanan infrastruktur jaringan yang digunakan. Penelitian ini menggunakan metode *action research* untuk menjelaskan keadaan dan situasi yang terjadi pada objek. Tahap-tahap yang dilakukan meliputi analisis level kematangan untuk mengukur sejauh mana proses pengamanan yang sudah dilakukan dan analisis kondisi keamanan infrastuktur jaringan yang digunakan. Pengambilan data level kematangan dengan menggunakan kuisioner, pengambilan data untuk mengukur kondisi keamanan infrastruktur menggunakan *form audit checklist* dengan memanfaatkan metode observasi langsung ke perangkat, untuk mengukur dari segi teknis pengamanannya dalam bentuk konfigurasi dasar pengamanan, selain itu penggunaan metode *penetration testing* digunakan untuk mengukur dari segi ketahanan keamanan software yang digunakan. Hasil dari penelitian ini berupa level kematangan dari prosedur pengamanan yang sudah dilakukan beserta kondisi keamanan infrastruktur saat ini. Kesimpulannya adalah Framework ISO 27001 sangat cocok digunakan untuk mengukur tingkat keamanan dari suatu sistem. *Penetration testing* sangat cocok digunakan untuk mengukur ketahanan suatu sistem dari berbagai resiko yang dapat mempengaruhi aspek keamanan menyangkut kerahasiaan, keutuhan dan ketersediaan informasi.

Kata kunci: ISO 27001, tingkat keamanan, level kematangan, penetration testing.

1. Pendahuluan

Keamanan jaringan menjadi sangat perlu dalam suatu penerapan prosedur jaringan komputer, mengingat dengan memanfaatkan koneksi jaringan maka dapat dengan mudah bertukar informasi [1]. Hal ini dapat menimbulkan resiko dalam bertukar informasi seperti mengambil atau memproduksi secara illegal, pembajakan dan lain-lain[2]. Sebelum melakukan pengamanan jaringan, sebaiknya dilakukan terlebih dahulu proses audit, agar sistem yang berjalan dapat diketahui celahnya sehingga untuk melakukan metode pengamanan jaringan lebih mudah [3].

Perlunya di terapkan keamanan informasi guna menjaga keamanan data dan informasi yang menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*)[4]. Dalam menerapkan optimalisasi keamanan jaringan terlebih dahulu dilaksanakan proses audit antara lain audit maturity level untuk mengetahui sejauh mana prosedur pengamanan yang telah dilakukan dan juga audit keamanan infrastuktur yang digunakan dari segi teknis konfigurasi keamanan jaringan, banyak framework yang digunakan oleh peneliti sebelumnya untuk menentukan tingkat kematangan yang ada pada suatu organisasi diantaranya adalah framework ISO/IEC, COBIT dan lain sebagainya[5].

ISO/IEC 27001:2005 adalah suatu sistem manajemen yang merujuk pada sistem keamanan informasi. Selain itu ISO/IEC 27001:2005 adalah salah satu standar yang berskala internasional untuk melakukan proses audit keamanan informasi pada suatu organisasi, mengukur tingkat keamanan sistem, serta dapat memaksimalkan sistem, guna mencapai suatu tingkat keamanan[6]. Selain itu dapat diartikan pula sebagai pendekatan sistematis untuk menetapkan , menerapkan , operasi, pemantauan , meninjau , memelihara dan meningkatkan keamanan informasi organisasi untuk mencapai tujuan bisnis[7].

2. Landasan Teori

Sebuah Sistem Manajemen Keamanan Informasi (SMKI) adalah pendekatan sistematis untuk menetapkan, menerapkan, operasi, pemantauan, meninjau, memelihara dan meningkatkan keamanan informasi organisasi untuk mencapai tujuan bisnis [7].

Sitem ini meliputi user, proses dan teknologi, untuk mengakui bahwa keamanan informasi tidak hanya tentang perangkat lunak antivirus, menerapkan firewall terbaru, keamanan komputer atau web server. Pendekatan secara keseluruhan untuk keamanan informasi harus strategis serta operasional , dan inisiatif keamanan yang berbeda harus diprioritaskan , terpadu dan lintas-referensi untuk memastikan efektivitas keseluruhan[7].

Tingkat kematangan merupakan gambaran kematangan proses teknologi informasi yang berlangsung pada sebuah perusahaan. Model kematangan dapat digunakan sebagai alat untuk melakukan benchmarking dan self-assessment oleh manajemen teknologi informasi untuk menilai kematangan teknologi informasi yang telah diimplementasikan [8].

Dengan model kematangan, manajemen dapat mengidentifikasikan hal-hal sebagai berikut.

1. Kinerja aktual dari perusahaan – posisi perusahaan saat ini [8].
2. Status industri saat ini – perbandingan [8].
3. Target perbaikan bagi perusahaan – ke mana perusahaan ingin dibawa [8].
4. Arah pengembangan yang diperlukan dari as-is menjadi to-be [8].

Konsep kematangan sistem informasi untuk menentukan sejauh mana penggunaan sistem informasi guna meningkatkan efisiensi, efektivitas, kualitas, dan respons konsumen. Dengan kematangan sistem informasi akan mempercepat perusahaan dalam merespons kepada perubahan lingkungan bisnis [8].

Model yang digunakan untuk mengendalikan proses teknologi informasi terdiri dari pengembangan suatu metode penilaian sehingga organisasi dapat melakukan evaluasi diri dari level non-existent dengan nilai 0 sampai dengan level optimized dengan nilai 5 [8].

Penetration testing adalah proses untuk mendapatkan akses ke sumber daya tentang username, password dan proses untuk mendapatkan informasi lainnya tanpa diketahui [9]. Penetration testing juga dapat diartikan sebagai proses untuk menguji kerentanan system dan menjelaskan apa saja yang bisa dilakukan seorang hacker jika system memiliki celah keamanan [10].

3. MetodePenelitian

Metode yang digunakan adalah metode *action research* yaitu menjelaskan tentang keadaan atau situasi yang terjadi. Tahap yang dilakukan adalah menggunakan kuisioner untuk mengukur level kematangan dari prosedur pengamanan yang sudah dilakukan. Kriteria penilaiannya di sesuaikan dengan kriteria penilaian CMM yang terdiri dari level 0 hingga level 5. Selanjutnya menggunakan *form audit checklist* untuk mengukur kondisi keamanan dari infrastuktur jaringan berupa mikrotik dan komputer.Kriteria penilaiannya adalah dengan menggunakan skala guttman, jawaban memiliki kriteria tegas yakni *yes or no.* selanjutnya akan dihitung persentase dari rata-rata setiap aspek yang dihitung berdasarkan hasil pengambilan data form audit dengan menggunakan rumus persentase :

$$x = \frac{JS}{\mathrm{SM}} \mathrm{x}\, 100\% \, [11]$$

Dimana :
X = Persentase pencapaian responden
JS = Jumlah keseluruhan skor yang di dapatkan
Sm = Skor Maksimal

4. Hasil

4.1. Analisis Maturity Level

Berdasarkan Data yang Diperoleh dari kuisioner maka tahap selanjutnya adalah mengukur *maturity level*-nya. Klausul ISO 27001 yang di ukur *maturity level*-nya adalah Klausul 11 yakni *Access Control* dimana data yang di dapat dari beberapa responden. Pada form kuisioner, responden diberikan beberapa pernyataan dan memilih jawaban pada kolom maturity level berdasarkan proses yang sesuai dengan level-level maturity sebagai berikut :

a) Level-0 = Tidak terdapat proses terkait sama sekali [12].
b) Level-1 = Tahap dimana manajemen sadar akan pentingnya proses terkait, tetapi implementasi yang terjadi masih bersifat reaktif, sesuai dengan kebutuhan mendadak yang ada dan tidak terorganisir [12].

c) Level-2 = Tahap dimana manajemen telah memiliki pola ataupun suatu perencanaan berdasarkan proses terkait [12].
d) Level-3 = Tahap Dimana Manajemen telah menciptakan dan mengkomunikasikan standar baku pengelolaan proses terkait meskipun belum diterapkan secara formal [12].
e) Level-4 = Tahap dimana manajemen telah menerapkan proses terkait secara formal dan terintegrasi [12].
f) Level-5 = Tahap dimana manajemen telah berkomitmen terhadap proses terkait agar dapat menjadi sebuah *best practice* yang selalu dikembangkan [12].

Tabel 1. Kerangka Kerja Perhitungan *Maturity Level*

A.11.5.3	**Sistem Manajemen Password**								
No	Pernyataan	Bobot	Maturity Level						Nilai
			0	1	2	3	4	5	
1	Apakah setiap operator yang memiliki hak untuk mengakses sistem manajemen router menggunakan password yang berkualitas, yakni penggabungan teks dan angka maupun simbol ?	1						x	5.00
2	Apakah password yang digunakan untuk akses manajemen router memiliki panjang karakter 8?	1		x					1.00
	Total Bobot	**2**	**Maturity Level**						**3.00**

Tabel 2. Hasil Maturity Level Responden 1

Klausul	Objektif Kontrol	Kontrol Keamanan	Maturity Level	Rata-rata
11. Access Control	11.1 Persyaratan Bisnis Untuk Pengendalian Akses	11.1.1 Kebijakan Pengendalian Akses	1.00	1.00
	11.2 Manajemen Akses User	11.2.1 Pendaftaran User	4.50	3.50
		11.2.2 Manajemen Hak Khusus	1.00	
		11.2.3 Manajemen Password User	3.50	
		11.2.4 Peninjauan terhadap hak Akses Pengguna Sistem	5.00	
	11.3 Tanggung Jawab User Terhadap Layanan Sistem	11.3.1 Penggunaan Password	5.00	4.33
		11.3.2 Perangkat Yang Di Tinggalkan Oleh User	5.00	
		11.3.3 Kebijakan Clear Desk/Clear Screen Sistem Informasi	3.00	
	11.4 Pengendalian Akses Jaringan	11.4.1 Kebijakan Penggunaan Layanan Jaringan	5.00	3.00
		11.4.2 Otentikasi User Untuk Koneksi Eksternal	2.00	
		11.4.3 Identifikasi Peralatan dalam Jaringan	5.00	
		11.4.4 Perlindungan terhadap remote diagnostic dan configuration port	5.00	
		11.4.5 Segregasi Dalam Jaringan	3.00	
		11.4.6 Pengendalian Koneksi Jaringan	1.00	
		11.4.7 Pengendalian Routing Jaringan	0.00	
	11.5 Pengendalian Akses Sistem Operasi	11.5.1 Prosedur Log-On yang aman	5.00	2.75
		11.5.2 Identifikasi dan Otentifikasi Pengguna	1.50	
		11.5.3 Sistem Manajemen Password	3.00	
		11.5.4 Penggunaan sistem utilities	5.00	
		11.5.5 Sesi Time-Out	1.00	
		11.5.6 Pembatasan Waktu Koneksi	1.00	

	A.11.6 Pengendalian Akses Aplikasi dan Informasi	A.11.6.1 Pembatasan Akses Informasi	5.00	5.00
		A.11.6.2 Isolasi Sistem Yang Sensitif	5.00	
	A.11.7 Mobile Computing and Teleworking	A.11.7.1 Mobile Computing dan Komunikasi	0.00	0.00
		A.11.7.2 Teleworking	0.00	
Jumlah				**19.58**
Maturity Level				**2.80**

Terlihat diatas untuk hasil maturity level klausul 11 pada responden 1 memiliki nilai 2.80. untuk rata-rata maturity level seluruh responden dapat dilihat pada tabel 3 dibawah ini :

Tabel 3. Hasil Maturity Level Keseluruhan Responden

Responden	ML
R1	2.80
R2	2.55
R3	2.53
Maturity Level	**2.62**

Dari hasil pada tabel 3 di atas didapatkan nilai dari rata-rata maturity level untuk klausul 11 bernilai 2.62 yang berarti berada pada level 2 dimana manajemen telah memiliki pola ataupun perencanaan untuk mengelola proses terkait [12].

4.2. Analisis Kondisi Keamanan Mikrotik dan Komputer

Perhitungan persentase aspek dapat dilihat pada tabel 4 dan tabel 5, dimana kolom Perangkat merupakan identitas komputer atau infrastruktur yang dilakukan pengujian, kolom SM berupa banyaknya butir-butir pernyataan yang ada pada form audit, kolom JS adalah jumlah dari butir-butir penyataan yang jawabannya bersifat “true” dan kolom persentase adalah perhitungan persentase dari jawaban berdasarkan hasil pengujian.

Tabel 4. Persentase Penilaian Kondisi Keamanan Mikrotik

Perangkat (n)	Skor Maksimal (SM)	JS	Persentase $x = \frac{JS}{\text{SM}} \text{x}\,100\%$
Mikrotik	24	13	54.17

Tabel 5. Persentase Penilaian Kondisi Keamanan Komputer

Perangkat (n)	Skor Maksimal (SM)	JS	Persentase $x = \frac{JS}{\text{SM}} \text{x}\,100\%$
PC1	35	24	68.57
PC2	35	17	48.57
PC3	35	24	68.57
PC4	35	13	37.14
PC5	35	17	48.57
PC6	35	22	62.86
PC7	35	15	42.86
PC8	35	24	68.57
PC9	35	17	48.57
PC10	35	24	68.57
PC11	35	24	68.57
PC12	35	19	54.29
PC13	35	23	65.71
Jumlah			751.42
Rata-Rata			57.80

Tabel 6. Contoh Penilaian Kategori keamanan

Persentase (%)	Kategori
0 - 20	Sangat Kurang

21 - 40	Kurang
41 - 60	Cukup
61 – 80	Baik
81 – 100	Sangat Baik

Terlihat pada tabel 6 di atas bahwa nilai dari persentase keamanan mikrotik berdasarkan hasil dari data form audit bernilai 54.17% dan persentase keamanan komputer bernilai 57.80% dan dapat dikategorikan Cukup berdasarkan kategori di atas.

4.3. Analisis GAP

Berdasarkan hasil wawancara ke beberapa responden yang bertanggung jawab untuk mengelola jaringan komputer pada instansi, didapatkan nilai kinerja potensial ataupun target yang ingin dicapai oleh instansi adalah posisi pada level 4 dimana manajemen telah menerapkan proses terkait secara formal dan terintegrasi. Dikarenakan pihak manajemen belum bisa melangkah ke level 5 Tahap dimana manajemen telah berkomitmen terhadap proses terkait agar dapat menjadi sebuah best practice yang selalu dikembangkan ketika level 4 tersebut belum terpenuhi secara keseluruhan. Berbeda dengan target kondisi dari keamanan infrastruktur yang digunakan, pihak manajemen menginginkan keamanan infrastuktur harus berada pada posisi 100%, dikarenakan keamanan dari infrastuktur harus terjamin keamanannya dari beberapa kelemahan yang dapat menjadi celah dari pihak tidak bertanggung jawab yang dapat merusak jaringan maupun data-data yang penting, ini sangat berpengaruh pada aspek keamanan yang menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) [4] informasi pada instansi.

Maka dari itu dapat di ukur tingkat kesenjangan berdasarkan hasil pengukuran *maturity level* keamanan jaringan, kondisi keamanan komputer serta kondisi keamanan mikrotik saat iniberdasarkan kinerja aktual yang telah di implementasikan dengan kinerja potensial atau target yang di inginkan. Pengukuran tersebut dapat dilihat pada tabel 7 di bawah ini :

Tabel 7. Kesenjangan kinerja aktual dengan kinerja potensial

Kategori	Kinerja Aktual	Kinerja Potensial	Kesenjangan
ML	2.62	4.00	1.38
KM	54.17%	100%	45.83%
KK	57.80%	100%	42.20%

Ket :
ML = Maturity Level KM
KM = Kondisi Keamanan Mikrotik
KK = Kondisi Keamanan Komputer

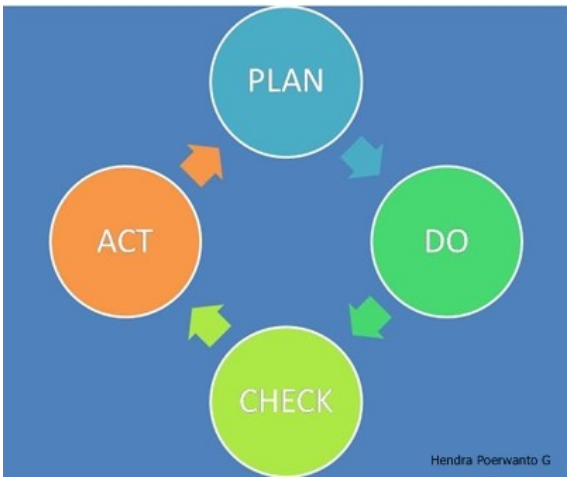
4.4. Optimalisasi

Dari hasil analisis GAP untuk maturity level di temukan kesenjangan antara kinerja aktual saat ini dengan kinerja potensial adalah 1.38, hal ini dikarenakan adanya temuan berupa SOP tentang pengamanan jaringan yang belum didokumentasikan sehingga tahap melakukan pengamanan masih bersifat individual berdasarkan pengetahuan dari administrator jaringan.

Selain itu adanya temuan beberapa proses yang tidak dilakukan sehingga untuk memenuhi syarat prosedur ISO 27001 belum bisa terpenuhi berdasarkan kategori domain yang tidak di penuhi. Hal ini perlu adanya SOP sehingga prosedur pengamanan jaringan dapat dilakukan secara terintegrasi berdasarkan syarat ISO 27001 serta dapat dilakukan berdasarkan konsep Plan-Do-Check-Act.

PDCA, singkatan bahasa Inggris dari "Plan, Do, Check, Act" (Rencanakan, Kerjakan, Cek, Tindak lanjuti), adalah suatu proses pemecahan masalah empat langkah iteratif yang umum digunakan dalam pengendalian kualitas [13].

PDCA dikenal sebagai “siklus Shewhart”, karena pertama kali dikemukakan oleh Walter Shewhart beberapa puluh tahun yang lalu. Namun dalam perkembangannya, metodologi analisis PDCA lebih sering disebut “siklus Deming”. Hal ini karena Deming adalah orang yang mempopulerkan penggunaannya dan memperluas penerapannya. Namun, Deming sendiri selalu merujuk metode ini sebagai siklus Shewhart, dari nama Walter A. Shewhart, yang sering dianggap sebagai bapak pengendalian kualitas statistis. Deming memodifikasi PDCA menjadi PDSA ("Plan, Do, Study, Act") untuk lebih menggambarkan rekomendasinya. Dengan nama apa pun itu disebut, PDCA adalah alat yang bermanfaat untuk melakukan perbaikan secara terus menerus tanpa berhenti [13].



Gambar 1. PDCA [13]

Selanjutnya Dari hasil GAP pengukuran kesenjangan kondisi keamanan komputer dan keamanan mikrotik saat ini dengan target yang ingin dicapai terlihat rata-rata berada pada 42-45% hal ini disebabkan adanya beberapa kerentanan tehadap aktivitas pencurian data, yang dapat dimanfaatkan oleh penyusup, diantaranya adalah penggunaan antivirus yang tidak ter-update sehingga *backdoor* tidak dapat terdeteksi oleh antivirus tersebut, selain itu adanya komputer yang masih menggunakan windows xp yang memiliki celah SMB netapi MS08-067, celah ini sangat mudah di exploitase menggunakan aplikasi metasploit sehingga seluruh data yang ada di dalamnya dapat dengan mudah diambil, dimodifikasi maupun di hapus.
Hal ini perlu diperbaiki sehingga aktivitas tersebut dapat dicegah, diantaranya penggunaan antivirus yang terupdate.karena penggunaan antivirus yang tidak terupdate kurang memadai sehingga tidak dapat mendeteksi *backdoor undetectable*.

Selain itu penggunaan windows xp yang rentan terhadap exploit dapat di update ataupun di ganti dengan sistem operasi windows terbaru, namun melihat perangkat keras yang digunakan tidak memenuhi syarat untuk instalasi windows terbaru maka celah tersebut dapat dicegah dengan menggunakan aplikasi firewall yang dapat memblokir aktivitas tersebut.

Pencegahan juga dapat dilakukan dari sisi wireless AP yang digunakan. Karena dari segi jaringan untuk mendeteksi celah komputer yang terhubung kejaringan lokal adalah melalui jaringan itu sendiri, teknik ini sering digunakan sebagai dasar untuk mendapatkan informasi kerentanan terhadap komputer. Teknik yang sering digunakan adalah TCP/IP scanner dengan memanfaatkan aplikasi NMAP, Zenmap scanner. Aplikasi ini dapat mendeteksi port yang terbuka serta dapat pula mendeteksi celah SMB netapi MS08-067. Pencegahan aktivitas scanner ini dapat dilakukan dengan mengkonfigurasi settingan *firewall* mikrotik sehingga aktivitas tersebut dapat di blokir.

5. Kesimpulan dan saran

5.1. Kesimpulan

Dari hasil penelitian tentang analisis keamanan jaringan dapat disimpulkan seperti berikut :

1. Hasil analisis *maturity level* pada Klausul 11 *Access Control* ISO 27001 terhadap prosedur pengamanan mikrotik, didapatkan nilai sebesar 2.62 yang berarti berada pada Level 2 yakni *repeatable but intuitive* dimana manajemen telah memiliki pola ataupun perencanaan untuk mengelola proses terkait.
2. Nilai kesenjangan antara kinerja aktual dan kinerja potensial yang bernilai 1.38 dari target 4.00
3. Terdapat temuan berupa SOP keamanan jaringan yang belum di dokumentasikan
4. Terdapat temuan beberapa proses yang belum dilaksanakan berdasarkan domain ISO 27001 khususnya pada Klausul 11
5. Hasil analisis persentase kondisi keamanan mikrotik saat ini berdasarkan penilaian dari hasil form audit bernilai 54.17 dan dapat dikategorikan Cukup
6. Nilai kesenjangan antara kinerja aktual dan kinerja potensial yang bernilai 45.83% dari target 100%
7. Hasil analisis persentase kondisi keamanan komputer saat ini berdasarkan penilaian dari hasil form audit bernilai 57.80 dan dapat dikategorikan Cukup

8. Nilai kesenjangan antara kinerja aktual dan kinerja potensial yang bernilai 42.20% dari target 100%
9. Terdapat beberapa temuan celah keamanan yang sangat berpengaruh terhadap kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*).
10. Framework ISO 27001 sangat cocok digunakan untuk mengukur tingkat keamanan dari suatu sistem
11. Penetration testing sangat cocok digunakan untuk mengukur ketahanan suatu sistem dari berbagai resiko yang dapat mempengaruhi aspek keamanan menyangkut kerahasiaan, keutuhan dan ketersediaan informasi

5.2. SARAN

Pada penelitian ini masih menggunakan proses pengukuran CMM maturity level sederhana. Maka dari itu diharapkan pada peneliti selanjutnya dapat menggunakan metode CMM lain untuk mengukur level kematangannya agar dapat dilihat perbandingannya.Pengujian Pentest dan observasi konfigurasi pengamanan software infrastuktur yang dilakukan masih bersifat pengujian standar maka diharapkan penelitian berikutnya dapat melakukan pengujian pentest dan observasi konfigurasi keamanan software yang lebih dalam mengenai keamanan.

Daftar Pustaka

[1] Masero, A. P. (2013). Perancangan pengelolaan jaringan it pada institut sains & teknologi akprind menggunakan teknologi vpn (*virtual private network*). . *ISSN:2338-6313*

[2] Mentang, R. (2015). Perancangan Dan Analisis Keamanan Jaringan Nirkabel Menggunakan *Wireless Intrusion Detection System* . *ISSN: 2301-8402.*

[3] Arief, M. R. (2008). *Auditing* Sistem Keamanan Jaringan. *p3m STMIK AMIKOM Yogyakarta*

[4] Utomo, M. (2012). Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I. *ISSN: 2301-9271*

[5] Noorhasanah. (2015). Evaluasi Tata Kelola Teknologi Informasi Berbasis *Framework Cobit* 5. *ISSN : 2302-3805*.

[6] Syahrial, H. (2014). Prototype Information Security Risk Assessment Tool Berbasis Lotus Notes Dalam Rangka Penerapan Sistem Manajemen Keamanan Informasi ISO 27001 . *ISBN: 979-26-0276-3*

[7] Governance, I. (2015, April 26). *ISO27001 and Information Security Training*. Retrieved from www.itgovernance.co.uk:http://www.itgovernance.co.uk/iso27001-information-security-training.aspx

[8] Tanuwijaya, H. (2013). Pengukuran Tingkat Kematangan Sistem Informasi Berdasarkan Critical Success Factors Pada Instalasi Rawat Inap Rumah Sakit Umum Surabaya . *ISSN 1979-3960*

[9] Northcutt, S. (2006). *Penetration Testing: Assessing Your Overall Security Before Attackers Do.*www.sans.org

[10] Pearson, A. (2014, Maret 20). *What is Penetration Testing and Why is It Important?* Retrieved from www.securityinnovationeurope.com: http://www.securityinnovationeurope.com/blog/what-is-penetration-testing-and-why-is-it-important

[11] Sugiyono. (2008). Memahami Penelitian Kualitatif*.* Bandung : Alfabeta

[12] Wibowo, M. P. (2008). Analisis Tingkat Kematangan (Maturity Level) Pengawasan dan Evaluasi Kinerja Teknologi Informasi Otomasi Perpustakaan Dengan Cobit *.Library indonesia university*.

[13] Poerwanto, H. (2012, Januari 16). *Plan-Do-Check-Act (PDCA)*. Retrieved from sites.google.com: https://sites.google.com/site/kelolakualitas/PDCA