RISTEKDIKTI

seminar nasional informatika 2017

PROSIDING

"e-Defense : Menjaga keamanan data menghadapi cyber warfare untuk memperkokoh kedaulatan Negara Kesatuan Republik Indonesia"

eDefense
seminar nasional informatika 2017

ISSN 1979-2328

Yogyakarta, 25 November 2017

SUSUNAN PANITIA

Penanggung Jawab : Dekan Fakultas Teknik Industri
Pengarah : 1. Wakil Dekan I FTI
2. Wakil Dekan II FTI
Ketua Umum : Ketua Program Studi Teknik Informatika
Wakil Ketua Umum : Sekretaris Program Studi Teknik Informatika

Ketua Pelaksana : Frans Richard Kodong, S.T., M.Kom.

Reviewer :
Assoc. Prof. Dr. Anton Satria Prabuwono, KSU
Dr. Tech. Ahmad Azhari UGM
Dr. Ir. Lukito Edi Nugroho, MT. UGM
Dr. Ashari SN, UGM
Ir. Balza Ahmad, M.Eng. UGM
Joko Siswantoro, Universitas Surabaya
Dr. Djoko Budianto, Atmajaya Yogyakarta
Dr. Slamet, Universitas Muhammadiyah Malang, Indonesia.
Dr. Abdul Kadir, STMIK Kartika Yani
Nuryono Setyo Widodo, S.T., M.T., Universitas Ahmad Dahlan
Dr. Herlina Jayadianti, S.T., M.T., UPN "Veteran" Yogyakarta
Hafsah, S.T., M.T., UPN "Veteran" Yogyakarta
Hidayatulah Himawan, S.T., M.M., M.Eng., UPN "Veteran" Yogyakarta
Bambang Yuwono, S.T., M.T., UPN "Veteran" Yogyakarta

Komite Pelaksana (Informatika UPN) :
Agus Sasmito Aribowo, S.Kom., M.Cs
Budi Santosa, S.Si.,M.T.
Dessyanto Boedi P, S.T.,M.T.
Frans Richard Kodong, S.T., M.Kom
Herry Sofyan, S.T., M.Kom.
Heriyanto, A.Md, S.Kom, M.Cs
Heru Cahya Rustamadji, S.Si.,M.T.
Juwairiah, S.Si., M.T.
Mangaras Yanu Florestiyanto, S.T., M.Eng
Nur Heri Cahyana, S.T.,M.Kom.
Oliver Samuel Simanjuntak, S.Kom, M.Eng
Paryati, S.T.,M.Kom.
Rifki Indra Perwira, S.Kom., M.Eng
Simon Pulung Nugroho, S.T.
Wilis Kaswidjanti, S.Si., M.Kom
Yuli Fauziah, S.T.,M.T.
Budi Cahyono
Pri Wahyu Eko Setiawan
Rahayu Ari Orbani.
Sugeng Rahmadi
Sukardi
Himpunan Mahasiswa Teknik Informatika (HIMATIF)

DAFTAR ISI

ANALISIS SISTEM MANAJEMEN KEAMANAN INFORMASI ELECTRONIC SECURITY SYSTEM (ESS) MENGGUNAKAN STANDAR ISO 27001 STUDI KASUS KANTOR PERWAKILAN BANK INDONESIA PROVINSI BALI

I Gede Putu Krisna Juliharta[1)], **I Made Maha Primananda Budi**[2)], **I Gusti Agung Lanang Agung Raditya**[3)]
STMIK Primakara
Jl. Tukad Badung No. 135 Renon – Denpasar, Bali
Email : krisna@primakara.ac.id [1)],coknanda32@gmail.com[2)], la.raditya27@gmail.com[3)]

Abstrak
Salah satu permasalahan dalam keseharian kegiatan dari sistem Electronic Security System (ESS) pada Bank Indonesia yaitu tidak adanya manajeman dalam keamanan informasi. Penelitian ini bertujuan untuk mengevaluasi tingkat kematangan sistem manajemen keamanan informasi ESS di Bank Indonesia Provinsi Bali. Metode yang digunakan adalah metode campuran kuantitatif dan kualitatif. Metode kualitatif diambil dari hasil kuesioner, wawancara dan studi dokumen dari hasil tersebut akan ditentukan tingkat kesenjangan (GAP analisis) terhadap tingkat kematangan saat ini dengan tingkat kemantangan yang diharapkan berdasarkan domain ISO 27001. Sedangkan metode kuantitatif diambil dari Business Impact Analysis (BIA). BIA dilakukan dengan penilaian jaringan sistem ESS dengan menggunakan metode Network Security Assessment. Dari hasil penelitian kualitatif menunjukan tingkat kematangan yang rata – rata berada pada level 5 (optimized), namun dari 11 domain yang dinilai ada 3 aspek domain yang berada pada level 4 (managed). Sedangkan hasil penelitian kuantitatif menunjukan bahwa BIA dalam penerapan jaringan pada server ESS memiliki 48 vulnerability dengan level resiko critical sebanyak 21, high sebanyak 5, medium sebanyak 20 dan low sebanyak 2 buah. Pada Client Main Badging memiliki 8 vulnerability dengan level resiko critical sebanyak 5, high sebanyak 1, medium sebanyak 1 dan low sebanyak 1 buah. Dan untuk Client Receptionist memiliki 4 vulnerability dengan level resiko critical sebanyak 1, high sebanyak 1, medium sebanyak 1 dan low sebanyak 1 buah. Untuk menutupi gap yang ada maka dilakukan rekomendasi perbaikan. Dan untuk hasil BIA dapat dijadikan acuan untuk membangun disaster recovery planning.

Kata kunci: *ISO 27001, Tingkat Kematangan, Tingkat Kesenjangan (GAP), Network Security Assessment, Business Impact Analysis.*

1. Pendahuluan

1.1 Latar Belakang

Informasi merupakan aset yang sangat bernilai bagi organisasi atau perusahaan. Dapat dikatakan Sistem Informasi (SI) sudah menjadi sebuah bagian dari perusahaan. Sistem informasi digunakan untuk mendukung berbagai kegiatan dalam perusahaan.

Keamanan informasi bertujuan untuk menjaga aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*). Ada beberapa framework yang dapat digunakan dalam penerapan sistem manajemen keamanan informasi antara lain NIST,GMITS, COBIT, ITIL, COSO, CISA, ISO 27001 [1]. Dari beberapa framework keamanan informasi yang ada, yang paling spesifik terhadap keamanan informasi adalah ISO 27001. ISO 27001 mencakup semua jenis organisasi (seperti perusahaan swasta, lembaga pemerintahan, dan lembaga nirlaba). ISO 27001 menjelaskan syarat-syarat untuk membuat, menerapkan, melaksanakan, memantau, menganalisa dan memelihara seta mendokumentasikan manajemen keamanan informasi dalam konteks risiko bisnis organisasi keseluruhan [2].

Dalam ISO 27001 keamanan sistem informasi tidak hanya berhubungan dengan penggunaan perangkat lunak antivirus, *firewall*, penggunaan *password* untuk komputer tetapi merupakan pendekatan secara keseluruhan baik dari sisi orang, proses dan teknologi untuk memastikan berjalannya efektivitas keamanan informasi.

Salah satu permasalahan dalam kegiatan dari sistem *Electronic Security System* ESS pada Bank Indonesia Provinsi Bali yaitu tidak adanya manajeman dalam keamanan informasi. Permasalahan yang ada pada Bank Indonesia Provinsi Bali terkait dengan standar manajemen keamanan informasi ISO 27001. Sehingga dengan

standar sistem manajemen keamanan informasi ISO 27001 diterapkan dalam manajemen informasi ESS diharapkan pimpinan dapat mengambil keputusan berdasarkan informasi yang akurat.

Berdasarkan latar belakang diatas, dibuatlah rumusan masalah dari penelitian yang akan dilakukan. Rumusan masalah dari penelitian ini adalah bagaimana mengevaluasi dan menganalisis sistem manajemen keamanan ESS di Bank Indonesia Provinsi Bali sehingga bisa diberikan rekomendasi perbaikan sesuai dengan standar ISO 27001.

Hasil output analisis sistem keamanan ESS meliputi tingkat kesenjangan (GAP) pada sistem ESS, lalu tingkat kesiapan terkait dengan *Business Impact Analysis* (BIA).

1.2 Tinjauan Pustaka

a. Definisi Sistem Manajemen Keamanan Informasi

Menurut SNI ISO/IEC 27001:2009 keamanan informasi adalah penjagaan kerahasiaan, integritas, dan ketersediaan informasi. Keamanan Informasi adalah terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) informasi (Tim Direktorat Keamanan Informasi) [3].

b. Definisi *Electronic Security System* (ESS)

ESS adalah sistem pengamanan lingkungan khusunya perkantoran yang terdapat di Bank Indonesia Provinsi Bali. Dimana fungsi ESS merupakan alat bantu dengan fungsi penginderaan dini, pemantau lingkungan dan pengendalian data [4]. Sistem yang terlibat dalam ESS meliputi *Access Control System* (ACS), *Security Alarm System* (SAS), *CCTV System*, *Fire Alarm System* (FAS).

c. Definisi ISO 27001

ISO 27001 merupakan standar keamanan informasi yang diterbitkan oleh *International Organization Standardization* dan *International Electrotechnical Commission* [5]. ISO 27001 mendefinisikan 39 buah kontrol objektif keamanan yang terstruktur dan dikelompokkan menjadi 11 domain keamanan informasi.

d. Definisi *Network Security Assessment*

Network Security Assessment merupakan metode penilaian pada suatu jaringan. Tujuan dari penilaian jaringan ini agar mengetahui tingkat *Vulnerability* (kerentanan) yang ada pada suatu jaringan sistem. Pengujian atau penilaian keamanan jaringan menggunakan network security tools yaitu Nessus dan Nmap.

1.3 Metode Penelitian

a. Tempat dan Waktu Penelitian

Tempat dan waktu penelitian dilakukan di Kantor Perwakilan Bank Indonesia Provinsi Bali, dimulai dari bulan Agustus 2017 hingga Oktober 2017.

b. Perancangan Penelitian

Dalam melakukan penelitian ini, penulis melakukan langkah – langkah penelitian sebagai berikut :

1. Pemilihan Masalah
   Penelitian dimulai dengan pemilihan masalah yang terjadi dilapangan, masalah yang dihadapi berasal dari temuan audit data yang dilakukan.
2. Studi Literatur
   Dari pemilihan masalah tersebut penulis mempelajari berbagai teori terkait tentang ISO 27001 dan *Network Security Assessment* yang akan digunakan dalam melakukan penelitian.
3. Menentukan ruang lingkup
   Dalam mementukan ruang lingkup ini, penulis menentukan apa saja yang akan dibahas sesuai dengan tema.
4. Pengumpulan data dan analisis risk assessment
   Data yang dikumpulkan pada penelitian ini terdiri dari penyebaran kuesioner, observasi, wawancara dan melakukan proses *network security assessment.* Setelah data terkumpul penulis melakukan analisis dari hasil kuesioner yang mengacu dengan ISO 27001 dengan hasil observasi dan wawancara. Sedangkan untuk *network security assessment* dilakukan analisis data yang didapat dari *network security tools.*
5. Pengolahan data
   Pada tahapan ini, penulis melakukan pengolahan data dari hasil observasi, wawancara, dan *Network Security Assesment*, dan *Business Impact Analysis.*
6. Menetapkan kontrol dan rekomendasi perbaikan
   Setelah melakukan proses pengolahan data maka selanjutnya dilakukan penetapan kontrol dan rekomendasi perbaikan berdasarkan standar ISO 27001.

2. Pembahasan

Dalam penyebaran kuesioner ISO 27001 didapat nilai rata – rata dari keseluruhan pernyataan yang disebar kepada responden. Rumus untuk menghitung hasil rata – rata maturity adalah sebagai berikut :

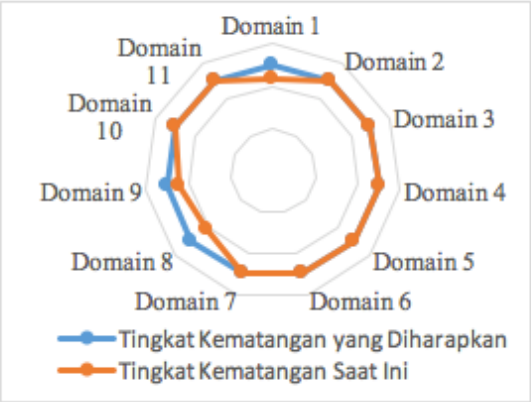
$$\text{Maturity} = \frac{\sum Rata - Rata \text{ Aktivitas}}{\text{Jumlah Soal}}$$

Selanjutnya setelah mendapatkan hasil tingkat kematangan saat ini dilakukan analisis untuk mengetahui tingkat level tiap domain. Untuk hasil tingkat maturity saat ini bisa dilihat pada Tabel 1 dibawah ini :

Tabel 1. *Rata – rata hasil maturity*

Domain ISO 27001	Maturity Saat Ini	Validasi Dokumen	Maturity yang diharapkan
Information Security Policies	4.33	4	5
Organization of Information Security	5	5	5
Human Resources Security	4.71	5	5
Asset Management	4.64	5	5
Access Control	4.64	5	5
Physical and Environment Security	4.92	5	5
Communication and Operations Management	4.61	5	5
System Acquisition Development and Maintenance	4.11	4	5
Information Security Incident Management	4.42	4	5
Business Continuity Management	5	5	5
Compliance	4.80	5	5
Rata – Rata	**4.63**	**5**	**5**

Berdasarkan nilai tingkat kematangan saat ini yang sudah diperoleh dari analisis kuesioner dan review dokumen serta wawancara maka masih terdapat kesenjangan di beberapa aspek domain. Dari gambar 1 bisa dilihat representasinya dalam bentuk grafik radar.



Gambar 1. *Hasil tingkat kematangan saat ini dengan tingkat kematangan yang diharapkan*

Dapat dilihat dari gambar 1 domain yang belum mencapai tingkat kematangan yang diharapkan, antara lain domain 1 *Information Security Policies,* Domain 8 *System Acquisition Development and Maintenance*,Domain 9 *Information Security Incident Management.*

Dari domain kesenjangan yang ada pada domain diatas memiliki tingkat kematangan yang belum tercapai maka dari itu akan dilakukan analisis dan diberikan rekomendasi perbaikan. Analisis yang dilakukan pada domain yang belum mencapai level diharapkan bisa dilihat pada Tabel 2 dibawah ini :

Tabel 2. *Tingkat Kesenjangan Domain yang belum mencapai level yang diharapkan*

Domain ISO 27001	Maturity Saat Ini	Maturity yang diharapkan	GAP (diharapkan- saat ini)
Information Security Policies	4.33	5	5 – 4.33 = 0.67
System Acquisition Development and Maintenance	4.11	5	5 – 4.11 = 0.89
Information Security Incident Management	4.42	5	5 – 4.42 = 0.58
Rata – rata			**0.71**

Dari tabel diatas bisa disimpulkan kesenjangan pada domain yang belum mencapi level yang diharapkan sebesar 0.71 atau dibulatkan menjadi 1. Dari nilai kesenjangan yang didapat diatas maka perlu dilakukan rekomendasi perbaikan dengan menyesuaikan masing – masing domain proses untuk mencapai level yang diharapkan. Untuk rekomendasi, berikut adalah kegiatan yang ahrus dilakukan agar bisa menutupi GAP yang ada adalah sebagai berikut :

1. Domain Information Security Policies
   - Mereview kembali kebijakan keamanan yang sudah di tetapkan sebelumnya.
   - Menetapkan aturan terhadap kebijakan yang sudah ditetapkan agar selalu dipatuhi dan diharuskan selalu melakukan review ualng tiap minggunya.
   - Membentuk struktur kerja untuk terus mengawasi pekerjaan dilapangan agar tetap mengacu pada kebijakan keamanan informasi.
   - Manajer terus mengontrol semua proses yang dilakukan agar sesuai dengan kebijakan informasi yang sudah ditetapkan.
2. Domain System Acquisition Development and Maintenance
   - Memberikan arahan kepada manajer dan user agar memahami tentang pentingnya keamanan informasi yang berguna untuk pengembangan sistem.
   - Memberi prosedur dalam tata cara memahami manajemen keamanan informasi.
   - Membuat loogbok sebagai bukti pengecekan sistem terlah dilakukan secara berkala.
   - Membuat jadwal untuk selalu update anti virus.
   - Menganalisa semua resiko yang mungkin terjadi.
3. Domain Information Security Incident Management
   - Membuat peraturan tentang pelaporan tiap insiden.
   - Pembuatan logbook untuk pencatatan tiap insiden.
   - Membentuk tim khusus dalam penanggulangan insiden yang terjadi.
   - Selalu memberikan arahan tentang pentingnya melaporkan tiap insiden yang ada.

Pada tahap selanjutnya penulis menjelaskan semua langkah dalam pengujian keamanan jaringan, mulai dari Target keamanan jaringan yang akan diuji, analisa kerentanan (*Vulnerabilities), Business Impact Analysis* dan *Risk Factor.*

a. Target keamanan jaringan yang akan diuji

Tabel 3 menjelaskan tentang informasi keamanan jaringan yang akan diuji oleh penulis.

Tabel 3. *Informasi Jaringan Target*

	Keterangan
Nama Jaringan	*Electronic Security System* (ESS)
Alamat	Jl. Letda Tantular No. 4 Denpasar Bali
Intansi	Kantor Perwakilan Bank Indonesia Provinsi Bali
Telp	(0361) 248982

b. Analisa kerentanan (*Vulnerabilities)*

Proses akhir dari *Network Security Assessment* adalah melakukan *vulnerability.* Perangkat yang diinvestigasi adalah perangkat hasil dari proses sebelumnya.

Tabel 4. *IP Address yang Dilakkan Analisa Kerentanan*

No	IP Address	Nama mesin
1	192.168.30.1	Server ESS
2	192.168.30.2	Client Main Badging
3	192.168.30.40	Client Receptionist

Tabel 4 diatas dapat digambarkan IP Address yang akan dilakukan proses scanning dengan tools Nessus untuk mendapatkan hasil kerentanan (*Vulnerability).*
Hasil kerentanan dapat dilihat di tabel 5 sampai tabel 7.

Tabel 5. *Kerentanan Server ESS*

No	Vulnerability	Jenis Kerentanan
1	Conficker Worm Detection (uncredentialed check)	Backdoors
2	HP System Management Homepage	Web servers
3	HP System Management Homepage Multiple Vulnerabilities	Web servers
4	Microsoft IIS 6.0 Unsupported Version Detection	Web servers

Tabel 6. *Kerentanan Client Main Badging*

No	Vulnerability	Jenis Kerentanan
1	Conficker Worm Detection (uncredentialed check)	Blackdoors
2	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution	Windows
3	MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution	Windows
4	MS09-001: Microsoft Windows SMB Vulnerabilities	Windows

Tabel 7. *Kerentanan Client Receptionist*

No	Vulnerability	Jenis Kerentanan
1	MS17-010: Security Update for Microsoft Windows SMB Server	Windows
2	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution	Windows
3	SMB Signing Disabled	MISC.
4	Multiple Ethernet Driver Frame Padding Information Disclosure	MISC.

Investigasi kerentanan atau *Vulnerability* merupakan tahap akhir dari *network security assessment.* Tabel 5 sampai tabel 7 merupakan hasil investigasi *vulnerability*, dengan hasil *vulnerability*, server ESS memiliki 48 *vulnerability*, client main badging sebanyak 8 *vulnerability*, client receptionist sebanyak 4 *vulnerability*. (analisa kerentanan secara keseluruhan ada pada lampiran 1). Dalam keamanan jaringan adanya *vulnerability* pada sistem menimbulkan resiko dan konsekuensi yang sangat besar terhadap *integrity, availability*, dan *confidentiality* dari keamanan jaringan dan sistem informasi.

c. *Business Impact Analysis* dan *Risk Factor*

Network Security Assessment selanjutnya adalah menghitung *Business Impact Analysis* (BIA). Proses BIA menggunakan penilaian CVSS versi 2 dengan skala yang disebutkan pada tabel 8.

Tabel 8. *Penilaian Level BIA*

Aturan Nilai	Level Risk Factor
0 <score< 4	Low
4 ≤ score< 7	Medium
7 ≤ score<10	High
10	Critical

Selanjutnya untuk hasil perhitungan BIA pada tiap *IP Address* bisa dilihat pada Tabel 9.

Tabel 9. *Business Impact Analysis Server ESS*

No	*Vulnerability*	AV	AC	Au	C	I	A	IS	ES	Score	Level
1	Conficker Worm Detection (uncredentialed check)	1.0	0.71	0.704	0.660	0.660	0.660	10	10	10	*Critical*
2	HP System Management Homepage	1.0	0.71	0.704	0.660	0.660	0.660	10	10	10	*Critical*
3	HP System Management Homepage Multiple Vulnerabilities	1.0	0.71	0.704	0.660	0.660	0.660	10	10	10	*Critical*
4	Microsoft IIS 6.0 Unsupported Version Detection	1.0	0.71	0.704	0.660	0.660	0.660	10	10	10	*Critical*
5	Microsoft Windows 2000 Unsupported Installation Detection	1.0	0.71	0.704	0.660	0.660	0.660	10	10	10	*Critical*
6	MS03-026: Microsoft RPC Interface Buffer Overrun	1.0	0.71	0.704	0.660	0.660	0.660	10	10	10	*Critical*
7	MS03-039: Microsoft RPC Interface Buffer Overrun	1.0	0.71	0.704	0.660	0.660	0.660	10	10	10	*Critical*
8	MS03-043: Buffer Overrun in Messenger Service	1.0	0.71	0.704	0.660	0.660	0.660	10	10	10	*Critical*

Dari tabel diatas bisa disimpulkan bahwa setiap IP Address yang dilakukan penilaian memiliki *vulnerability*. *Business Impact Analysis* dari masing – masing IP terdapat tingkkatan level *Critical, High, Medium, Low.*(Hasil *Business Impact Analysis* secara keseluruhan ada pada lampiran 1). Hasil *vulnerability* secara keselurhan bisa dilihat pada tabel 10.

Tabel 10. *Total hasil vulnerability*

No	Nama IP Jaringan	Jumlah *Vulnerability*
1	Server ESS	48
2	Client Main Badging	8
3	Client Receptionist	4

Untuk melihat secara detail hasil jumlah *vulnerability* yang dihasilkan bisa dilihat pada Tabel 11. (Hasil *vulnerability* secara keseluruahan ada pada lampiran 1).

Tabel 11. *Hasil Analisis dan Evaluasi Vulnerability berdasarkan Business Impact Analysis*

No	Nama IP Jaringan	Level Resiko			
		Critical	High	Medium	Low
1	Server ESS	21	5	20	2
2	Client Main Badging	5	1	1	1
3	Client Receptionist	1	1	1	1

Hasil yang didapat dari penilaian keamanan jaringan pada sistem ESS di Bank Indonesia Provinsi Bali, didapat hasil tingkat resiko *critical* sebanyak 27 buah, tingkat resiko *high* sebanyak 7 buah, tingkat resiko *medium* sebanyak 22 buah dan tingkat resiko *low* sebanyak 4 buah.

3. Kesimpulan

Hasil dari penelitian yang telah dilakukan didapat kesimpulan sebagai berikut :

a. Dalam penelitian yang dilakukan terhadapat hasil yang kontradiksi antara data obyektif dengan data subyektif.
b. Hasil data subyektif menunjukan maturity tingkat kematangan telah mencapai hasil yang diharapkan dengan ditunjukkan pada nilai kematangan pada tiap IP jaringan ESS dengan mesin server ESS dengan

nilai kematangan 5 (optimized), mesin Client Main Badging dengan nilai kematangan 5 (optimized) dan mesin Client Receptionist dengan dengan nilai kematangan 5 (optimized).

c. Hasil data obyektif yang dilakukan dengan *Network Security Assessment* terdapat perbedaan dengan hasil data subyektif dengan menunjukan hasil pada pada mesin server ESS memiliki level resiko sebanyak 21 buah level critical, 5 buah level high, 20 buah level medium dan 2 level low. Pada mesin Client Main Badging memiliki level resiko sebanyak 5 buah level critical, 1 buah level high, 1 buah level medium dan 1 buah level low, sedangkan pada mesin Client Receptionist memiliki level resiko sebanyak 1 buah level critical, 1 buah level high, 1 buah level medium dan 1 buah level low.

Dari hasil kesimpulan diatas peneliti memiliki beberapa saran yang dapat dipertimbangkan untuk pengembangan sistem pada ESS. Adapun saran yang dimaksud adalah sebagai berikut :

a. Rekomendasi perbaikan yang diberikan agar dilakukan untuk pengembangan sistem.
b. Hasil *Business Impact Analysis* dapat dijadikan acuan untuk membangun *disaster recovery planning.*
c. Dalam penerapan sistem keamanan jaringan pada sistem ESS di kpw BI Provinsi Bali diharapkan adanya komunikasi dalam hasil obyektif dalam wawancara dengan hasil subyektif yang terdapat dilapangan agar tidak terjadi kontradiksi.
d. Pada penelitian selanjutnya diharapkan melakukan analisis sistem manajemen keamanan informasi dengan domain yang berbeda dan dilakukan ditempat lain.

Daftar Pustaka

[1] Rizal," Macam–macam Framework Audit IT", 30 Desember 2016, *https://www.researchgate.net/publication/311972151* diakses pada tanggal 30 desember 2016.
[2] Zulfikar, Reza, 2013, "Audit Kepatuhan Keamanan Informasi Dengan Menggunakan Framework ISO 27001.", Jakarta.
[3] Direktorat Badan Standarisasi Nasional, 2009. SNI ISO/IEC 27001:2009 Teknologi Informasi-Teknik Keamanan-Sistem Manajemen Keamanan Informasi-Persyaratan. Jakarta: Badan Standarisasi Nasional.
[4] Bank Indonesia, 2005, "*Sistem Pengamanan Bank Indonesia (SISPAMBI) Nomor : 7 / 9 / PDG / 2005"*, Jakarta: Bank Indonesia.
[5] Rosmiati, 2016, "Analisis Keamanan Informasi Kebutuhan Teknikal dan Operasional Mengkombinasikan Standar ISO 27001 pada Kantor Biro Teknologi Informasi.", Yogyakarta, Jurnal Buana Informatika, Vol 6, No.4