Penilaian Keamanan Jaringan Menggunakan Standar ISO/IEC 27001 Pada Kantor Redaksi Harian Suara Merdeka

Network Security Evaluation Using Standard ISO / IEC 27001 In the Editorial Office Suara Merdeka

Rian Adi Surya[1], MY. Teguh Sulistyono, M.Kom[2]
[1,2]Sistem Informasi, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang
[1,2]Jl. Nakula I, No. 5-11, Semarang, Kode Pos 50131, Telp. (024) 3515261, 3520165 Fax: 3569684

Abstrak

ISO / IEC 27001: 2005, standar untuk Sistem Manajemen Keamanan Informasi (SMKI), adalah pendekatan sistematis untuk mengelola informasi sensitif perusahaan sehingga tetap aman, meliputi orang, proses dan sistem IT. Dengan penerimaan standar internasional, organisasi sekarang dapat mengembangkan dan menerapkan kerangka kerja global untuk mengelola keamanan informasi mereka. standar dapat digunakan oleh berbagai organisasi mulai dari organisasi kecil, menengah dan hingga organisasi besar. ISO / IEC 27001: 2005 menetapkan proses untuk memungkinkan organisasi atau perusahaan untuk menetapkan, menerapkan, mengkaji dan memonitor, mengelola dan memelihara information security management system (ISMS) secara efektif dengan siklus Plan-Do-Check-Act dan penelitan tindakan (Action Research) sehingga dapat dijadikan kebutuhan untuk perbaikan secara terus-menerus. PT. Suara Merdeka Press merupakan suatu perusahaan yang bergerak dibidang media cetak maupun elektronik yang membutuhkan keamanan informasi baik berupa bentuk digital maupun visual. Guna menjaga keamanan informasi diperlukan suatu manajemen informasi yang matang sehingga memerlukan suatu evaluasi untuk mengetahui kondisi keamanan jaringan dalam kondisi baik atau buruk. Dengan memanfaatkan Klausul pengelolaan aset, keamanan sumber daya manusia, keamanan fisik dan lingkungan, akses kontrol serta manajemen insiden keamanan informasi pada ISO/IEC 27001:2005 dihasilkan temuan yang bermanfaat bagi PT. Suara Merdeka Press guna mengevaluasi sistem manajemen keamanan informasi yang sudah ada

Kata kunci— *ISO / IEC 27001:2005, Sistem Manajemen Keamanan Informasi (SMKI), information security management system (ISMS), Action Research, Klausul.*

Abstract

ISO / IEC 27001: 2005 standard for Information Security Management System (ISMS) is a systematic approach to managing sensitive company information so that it remains safe, encompassing people, processes and IT systems. With the acceptance of international standards, organizations are now able to develop and implement a global framework for managing the security of their information. standards can be used by organizations ranging from small organizations, medium and up to large organizations. ISO / IEC 27001: 2005 establishes a process to allow the organization to establish, implement, review and monitor, manage and maintain the information security management system (ISMS) effectively with the Plan-Do-Check-Act and research actions (Action Research) so it can be used as the need for continuous improvement. PT. Suara Merdeka Press is a company engaged in the electronic and print media

who need the security of information such as digital and visual form. In order to maintain the security of information required a mature information management so requires an evaluation to determine the condition of the network security is in good condition or bad. By utilizing Clause asset management, human resources security, physical and environmental security, access control and information security incident management ISO / IEC 27001: 2005 is produced findings that are beneficial for PT. Suara Merdeka Press to evaluate the information security management system that already exists.

Keywords— *ISO / IEC 27001: 2005 Information Security Management System (ISMS), information security management system (ISMS), Action Research, Clause.*

1. PENDAHULUAN

PT. Suara Merdeka Press adalah media cetak yang didirikan pada tanggal 11 Februari 1950 oleh H. Hetami dengan ruang lingkup pemasaran di Jawa Tengah dan Daerah Istimeda Yogyakarta, Pendiri Harian Suara merdeka mempunyai misi awal memperdengarkan suara rakyat yang baru saja merdeka. Hal tersebutlah yang dijadikan pertimbangan pemberian nama yang sebelumnya direncanakan oleh pendiri Mimbar Merdeka. Pada tahun 1982 PT. Suara Merdeka Press Semarang didirikan.

Awal pendirian surat kabar ini hanya dikelola secara sederhana dengan dua orang wartawan dan dua meja serta dua mesin ketik, harian Suara Merdeka terdiri dari empat halaman dan dicetak dengan oplah 5000 eksemplar, karena belum mempunyai percetakan sendiri, Harian Suara Merdeka menumpang cetak korannya di Harian *De Locomotief* yang beralamat di jalan Kepodang, Semarang.

Dengan permintaan publik akan koran Harian Suara Merdeka meningkat dan perkembangan perusahaan begitu pesat dan mampu mendirikan perusahaan percetakan dengan nama Masscom Graphy yang beralamat di Jl. Raya Kaligawe KM 5, Semarang.

Pada Tahun 1992 PT. Suara Merdeka Press Semarang memasuki babak baru dengan menggunakan tekhnologi *lay outer* dengan menggunakan mesin *Macintosh* dan produksi koran saat ini sudah mencapai 200.000 eksemplar per hari. Suara Merdeka telah mengalami tiga kali masa kepemimpinan yaitu, H. Hetami (generasi pertama tahun 1950-1982), Ir. Budi Santoso (generasi ke-dua tahun 1982-2010, beliau adalah menantu dari H. Hetami), dan Kukrit Suryo Wicaksono, MBA. (generasi ke-tiga tahun 2010- sekarang, beliau adalah putra sulung dari Ir. Budi Santoso).

Dengan perkembangan teknologi sekarang ini perlunya akan suatu sistem keamanan yang mumpuni agar keamanan jaringan komputer pada kantor Redaksi Suara Merdeka sangat diperlukan karena keamanan data, informasi dan materi berita tidak disalah gunakan oleh oknum yang tidak bertanggung jawab.

Keamanan informasi pada kantor Redaksi Suara Merdeka sangat diperlukan karena menyangkut tentang keamanan informasi perusahaan yang sangat rahasia. Informasi itu berbentuk digital, visual (video, diagram), ditampilkan di website, dan sebagainya. Apapun bentuk informasi yang disajikan, informasi tersebut harus selalu aman. Salah satu permasalahan dalam keseharian kegiatan dari devisi Redaksi ditemukannya user dipakai oleh orang lain untuk pengolahan berita, disini mengingat pentinggnya keamanan informasi, maka kebijakan tentang keamanan informasi harus baik dan setidaknya harus mencakup beberapa prosedur seperti prosedur pengelolaan aset, prosedur pengelolaan sumber daya manusia, prosedur pengamanan

fisik dan lingkungan, prosedur pengamanan logical security, prosedur pengamanan operasional teknologi informasi dan prosedur penanganan insiden dalam pengamanan informasi. Untuk itu diperlukan evaluasi keamanan sistem manajemen informasi untuk memastikan keamanan informasi diterapkan sesuai dengan prosedur. Standar yang digunakan dalam manajemen keamanan informasi adalah ISO/IEC 27001. ISO/IEC 27001 dipilih karena standar ini sangat fleksibel dikembangkan karena sangat tergantung dari kebutuhan organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis dan jumlah pegawai dan ukuran struktur organisasi.

ISO/IEC 27001 merupakan dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) atau Information Security Management System (ISMS) atau SNI ISO/EIC 27001:2009 yang dikeluarkan oleh Kominfo Republik Indonesia yang memberikan gambaran secara umum mengenai apa saja yang seharusnya dilakukan dalam usaha pengimplementasian konsep-konsep keamanan informasi pada sebuah organisasi.

Uraian-uraian di atas maka penulis bermaksud untuk mengangkat permasalahan tersebut sebagai bahan penelitian ini. Adapun judul yang dipilih yaitu ”Evaluasi Keamanan Jaringan Menggunakan Standar ISO/IEC 27001 pada Kantor Redaksi Harian Suara Merdeka”. Berdasarkan latar belakang yang ada, maka penulis ingin merumuskan permasalahan yang ada yaitu “Seberapa baik manajemen keamanan informasi pada Kantor Redaksi Harian Suara Merdeka menggunakan standar ISO/IEC 27001?”. tujuan dari penelitian ini adalah :

1. Mampu menerapkan tata kelola keamanan informasi secara efektif, efisien, dan konsisten.
2. Membuat evaluasi terhadap sistem yang diterapkan sehingga dapat memberikan solusi terbaik terhadap sistem tersebut dan memberikan rekomendasi perbaikan untuk meningkatkan tingkat kelengkapan dan tingkat kematangan keamananiInformasi pada bagian IT Kantor Redaksi Harian Suara Merdeka.

Penelitian sebelumnya telah dilakukan berdasarkan framework ISO/IEC 27001. Diantaranya adalah penelitian yang dilakukan oleh Lussianty, dkk, penelitian tersebut membahas tentang pengukuran risiko pada PT. Street Directory Indonesia dengan judul penelitian “*Pengukuran Risiko Informasi Teknologi Pada PT. Street Directory Indonesia dengan Menggunakan ISO/IEC 27001/2”* penelitian tersebut dilakukan untuk mengidentfikasi praktek keamanan dan memberikan solusi untuk mengelola keamanan informasi dan meminimalisir dapak risiko yang terdapat pada PT. Street Directory Indonesia. [1]. Penelitian lainnya dilakukan oleh Riawan Arbi Kusuma yang membahas tentang keamanan system informasi dengan judul *“Audit Keamanan Sistem Informasi Berdasarkan Standar SNI-ISO 27001 Pada Sistem Informasi Akademik Universitas Islam Negeri Sunan Kalijaga Yogyakarta”* [2]. Penelitian tersebut dilakukan untuk memformulasikan hasil audit keamanan Sistem Informasi Akademik UIN SUNAN KALIJAGA YOGYAKARTA dengan menggunakan standar SNI ISO 27001.

ISO/IEC 27001 adalah sebuah metode khusus yang terstruktur tentang pengamanan informasi yang diakui secara internasional. Standar ISO/IEC 27001 merupakan dokumen standar sistem manajemen keamanan informasi atau Information Security Management Syestem, biasa disebut ISMS yang diterbitkan pada bulan Oktober 2005 oleh International Organization for Standarization dan International Electrotechnical Commission yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah perusahaan dalam usaha mereka untuk mengevaluasi, mengimplementasikan dan memelihara keamanan informasi di perusahaan berdasarkan “best practise” dalam pengamanan informasi.

Adapun 11 klausul dari ISO/IEC 27001 yaitu :

A.5. Security policy (kebijakan keamanan informasi)
A.6. Organization of information security (Organisasi keamanan informasi)
A.7. Asset management (Manajemen aset)

A.8. Human resources security (Keamanan sumber daya manusia)
A.9. Physical and environmental security (Keamanan fisik dan Lingkungan)
A.10. Communications and operations management (Manajemen Komunikasi dan Operasi)
A.11. Access control (Akses kontrol)
A.12. Information system acquisition, development, and maintenance (Pengadaan/akuisisi, pengembangan dan pemeliharaan sistem informasi)
A.13. Information security incident management (Manajemen insiden keamanan informasi)
A.14. Business continuity management (Manajemen kelangsungan usaha)
A.15. Compliance (Kesesuaian)

2. METODE PENELITIAN

Metode penelitian yang digunakan adalah metode kuantitatif. Menurut Tuban (2001) metode kuantitatif adalah ilmu dan seni yang berkaitan dengan tata cara (metode) pengumpulan data, analisa data, dan interpretasi hasil analisis untuk mendapatkan informasi guna penarikan kesimpulan dan pengambilan keputusan.

a. Metode Pengumpulan Data

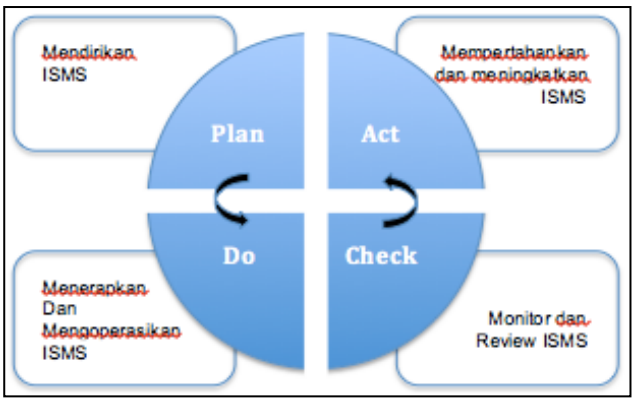
Dalam penelitian ini metode pengumpulan data yang dilakukan di Kantor Redaksi Harian Suara Merdeka yang beralamatkan di Jalan Raya Kaligawe KM 5 Semarang akan dimulai pada 29 Februari 2016 adalah adalah dengan menggunakan dua metode yaitu data primer dan sekunder, data primer yaitu :

1. Observasi
   Dengan mengadakan peninjauan langsung ke Kantor Redaksi Harian Suara Merdeka yang merupakan pusat sistem informasi dan data dengan mengamati, mencatat dan menganalisis keamanan informasi yang ada di Kantor tersebut dan bagaimana mengamankan sistem keamanan informasi menggunakan standar ISO/IEC 27001 pada Kantor Redaksi Harian Suara Merdeka.
2. Wawancara
   Mendapatkan data secara langsung dari sumber yang mengerti sehubungan dengan pengamatan yang lakukan dengan mengajukan pertanyaan-pertanyaan kepada karyawan yang berada di Kantor Redaksi Harian Suara Merdeka yang bertugas sebagai *administrator* pada instansi tersebut.
3. Angket (*Quisioner*)
   Pengumpulan data yang dilakukan dengan cara memberikan seperangkat pertanyaan atau pernyataan kepada orang yang dijadikan responden dan responden diminta untuk menjawab atau mengisi pertanyaan/pernyataan tersebut.

Sedangkan data sekunder diperoleh dengan melakukan *Study literature* yang *relevan*, yaitu dengan cara mempelajari buku dan jurnal yang diperoleh / dikumpulkan dan disatukan oleh studi-studi sebelumnya atau yang diterbitkan oleh berbagai instansi lain. Biasanya sumber tidak langsung berupa data dokumentasi dan arsip-arsip resmi.yang berkaitan dengan penulisan penelitian

b. Pengolahan Data

PLANT – DO – CHECK – ACT (PDCA) diterapkan pada struktur keseluruhan proses Sistem Manajemen Keamanan Informasi. Model PDCA dalam proses Sistem Manajemen Keamanan Informasi.



Gambar 3.1 Proses SMKI

c. Ruang Lingkup

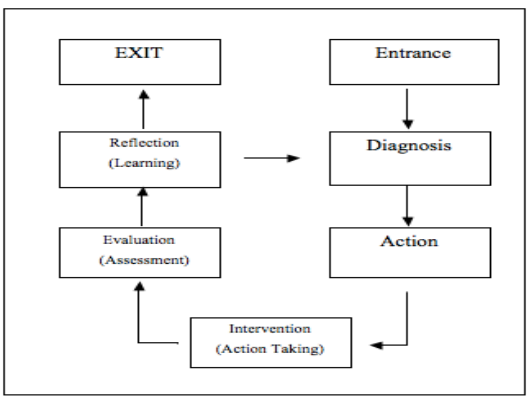
Ruang lingkup yang akan dilakukan dengan melakukan observasi, wawancara dan kuesioner, dalam pedoman untuk menerapkan manajemen resiko dalam penggunaan TI dan disesuaikan dengan kriteria audit yang menggunakan standar ISO 27001. Tabel 3.1 merupakan pemetaan dari pedoman yang digunakan terhadap klausul-klausul ISO 27001.

tabel 3.1 Ruang Lingkup Klausul

Diskripsi	Klausul
Pengelolaan Aset	7
Keamanan Sumber Daya Manusia	8
Keamanan Fisik dan Lingkungan	9
Akses kontrol	11
Manajemen insiden keamanan informasi	13

3. HASIL PENELITIAN DAN PEMBAHASAN

Tahapan dalam melakukan penelitian menggunakan *Action Research,* yaitu :



Gambar. 3.1. *Action Research Work Flow*

a. Entrance

Menentukan obyek yang dipakai sebagai titik mulainya penelitian atau audit. Obyek penelitian penulis pilih adalah PT. Suara Merdeka Press khususnya Kantor Redaksi Harian Suara Merdeka yang berkantor pada Jalan Raya Kaligawe KM 5 Semarang.

b. Diagnosis

Diagnosa tersebut menyangkut Konsep dasar dari keamanan teknologi informasi yaitu :

1) Kerahasiaan, informasi yang dilindungi dan mempunyai sifat rahasia terhadap keterbukaan dari oknum yang tidak berkepentingan yang tidak berhak akan informasi tersebut. Apakah karahasiaan terhadap akses kontrol aplikasi, jaringan, server serta data terjaga dengan baik.
2) Integritas, data haruslah komplit dan tidak diubah, disini apa terjadi perubahan terhadap data dimana data hanya bisa diakses oleh yang mempunyai hak akses terhadap data tersebut.
3) Ketersediaan, tersedianya data dan informasi bagi pengguna jika diperlukan. Apakah data yang sudah terpakai masih ada ?

faktor utama dalam perlindungan keamanan yang perlu dipertimbangkan,

1) Keamanan sistem TI
2) Keamanan jaringan dan koneksi internet
3) Penggunaan mekanisme keamanan dengan menggunakan password dan enkripsi
4) Pendekatan sistemtis atas keamanan TI
5) Faktor sumber daya manusia
6) Perlindungan atas bencana alam dan kebakaran
7) Perawatan aset TI

c. Action Planing

Ruang lingkup audit keamanan sistem informasi berdasarkan pedoman untuk penerapan management resiko yang digunakan berdasarkan standart ISO 27001. Berikut merupakan pemetaan dari pedoman Klausul-klausul ISO 27001 yang digunakan dalam Audit pada Suara Merdeka Press.

Tabel 3.1 Ruang Lingkup Klausul

Diskripsi	Klausul
Pengelolaan Aset	7
Keamanan Sumber Daya Manusia	8
Keamanan Fisik dan Lingkungan	9
Akses kontrol	11
Manajemen insiden keamanan informasi	13

d. Action Taking

Pelaksanaan Audit menghasilkan bukti, temuan dan nilai tingkat kematangan dari tiap-tiap kontrol keamanan. Pendokumentasian berupa wawancara diperoleh saat prosedur pembuatan pertanyaan dari pertanyaan yang sebelumnya telah dibuat. Bukti-bukti diperoleh dari wawancara kemudian hasil dari temuan dievaluasi dan dianalisa sehingga dapat ditentukan nilai dari tingkat kemampuan dari masing-masing kontrol keamanan.

Dalam penyusunan prioritas risiko, frekuensi atau probabilitas dampak dari masing – masing risiko diberi bobot nilai antara 0 sampai dengan 3. Untuk probabilitas risiko

Tabel. 3.2 Frekuensi dari Probabilitas

Probabilitas	Dampak	Nilai
Tidak ada	Dapat menghancurkan sistem	0
Kesadaran Rendah	Dampak pada kerusakan finansial	1
Kesadaran Sedang	Dampak dapat diukur, diperlukan usaha untuk perbaikan	2
Kesadaran Tinggi	Tidak memiliki dampak pada sistem	3

Untuk memetakan pertanyaan berdasarkan Jobdesk masing-masing perlu di buat Master Control, Master Question, dan Form Question.

Contoh tabel Form Master Control

Tabel. 3.3 form Master Control

No	Klausul	Diskripsi	Audite
1	A.7	Pengelolaan Aset	
	A.7.1	Tanggung jawab terhadap aset	Koordinator IT
	A.7.2	Klasifikasi informasi	Koordinator IT

Contoh tabel Form Mater Question

Tabel. 3.4 form Master Question

Klausul	Kode	Pertanyaan
A.7		
A.7.1	Q1	Aset dalam sistem meliputi apa saja?
	Q2	Sudahkan dilalukannya inventarisasi terhadap aset?
	Q3	Siapa yang melakukan pengelolaan aset?
	Q4	Bagaimana kebijakan dalam pengelolaan aset?
	Q5	Siapakah yang bertanggung jawab terhadap pendataan aset?
	Q6	Sudahkan dilakukannya pelabelan pada masing-masing aset?
	Q7	Siapa yang memberi label pada masing-masing aset?
	Q8	Apakah pemberian label pada masing-masing devisi berbeda?
	Q9	Apakah ada pelabelan khusus untuk beberapa aset?
	Q10	Bagaimana proses pelabelan aset tersebut?

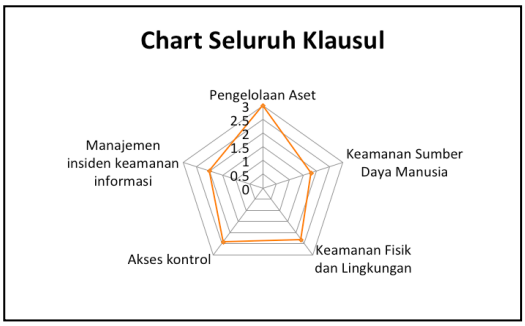
e. Evaluating

Hasil audit keamanan sistem informasi berupa temuan dan rekomendasi untuk perusahaan Suara Merdeka. Temuan tersebut diperoleh dari evaluasi dan analisa di lapangan, temuan-temuan tersebut digunakan sebagai perbaikan kontrol keamanan.

Tabel 3.5 Hasil seluruh Klausul

Klausul	Nilai Rata-rata
Pengelolaan Aset (Klausul 7)	3
Keamanan Sumber Daya Manusia (Klausul 8)	1,8
Keamanan Fisik dan Lingkungan (Klausul 9)	2,3
Akses control (Klausul 11)	2,4
Manajemen insiden keamanan informasi (Klausul 13)	2

representasi nilai rata-rata Klausul



Gambar 3.2. Representasi nilai rata-rata Klausul

Hasil dari tiap-tiap klausul dan ketika dilakukannya analisa dan evaluasi dari audit Keamanan Sistem Informasi pada PT. Suara Merdeka Press dapat dipaparkan beberapa kondisi yang telah sesuai dengan kontrol keamanan pada ISO 27001, beberapa kondisi tersebut yaitu :

1. Terdapatnya aturan mengenai tanggung jawab keamanan informasi
2. Terdapat dan sesuainya ruang dimana Server di tempatkan
3. Terdapat dokumentasi terhadap prosedur operasi
4. Ditemukan kebijakan tentang bina norma-norma keselamatan bagi para pekerja oleh Direktorat Bina Norma-norma Keselamatan Kerja & Hyperkes.
5. Ditemukan hak akses ruang server oleh para staf TI dan orang-orang lain yang berkepentingan.

Sedangkan kondisi yang masih perlu untuk dilakukannya perbaikan, yaitu :

1. Pada klausul 7 yaitu Pengelolaan Aset tidak perlu dilakukannya perbaikan karena kesadaran akan pendokumenasian atau pengelolaan aset memiliki kesadaran yang tinggi sehingga tidak memiliki risiko pada sistem.
2. Pada Klausul 8 yaitu Keamanan Sumber Daya Manusia perlu adanya perbaikan dan diadakannya pelatihan bertahap guna memberi bekal kepada user yang berkompeten pada devisinya sehingga tidak menghambat sistem karena berdampak fatal terhadap kelangsungan bisnis.

3. Pada klausul 9 yaitu Keamanan Fisik dan lingkungan perlu memberi pengarahan akan bahaya asap rokok terhadap peralatan elektronik khususnya seperti komputer, dan perangkat jaringan lainnya.
4. Pada klausul 11 yaitu Akses kontrol, Staff it perlu mengupdate user dan password pada devisi Redaksi serta memberikan sosialisasi kepada Redaksi tentang pentingnya hak akses otorisasi terhadap akses kontrol terutama penggunaan user dan password pada sistem.
5. Pada klausul 13 yaitu Menejemen Insiden Keamanan Informasi perlu adanya penanganan terhadap server dengan memperkuat Firewall pada server dan mengupayakan penyeragaman operating system pada server mengingat server pernah terkena Phising, Hijack.

4. KESIMPULAN

Dari temuan-temuan dan hasil dari pengolahan dapat ditarik beberapa kesimpulan yaitu :

a. Langkah audit keamanan informasi dilakukan pembuatan pernyataan, penentuan nilai bobot, dan penentuan nilai kematangan sehingga perencanaan audit menghasilkan identifikasi ruang lingkup dalam menerapkan manajemen resiko.
b. Audit pada PT. Suara Merdeka Press sesuai dengan yang diharapkan sebelumnya dimana nilai dari Klausul yang telah disepakati sebelumnya, dimana Klausul Pengelolaan Aset memiliki nilai rata-rata yang paling m,ltinggi dengan nilai rata-rata 3, sedangkan Klausul dengan nilai rata-rata yang sangat kurang terdapat pada Klausul ke 8 yaitu Keamanan Sumber Daya Manusia dengan nilai rata-rata 1,8.

c. Secara Keseluruhan audit dengan klausul yang telah disepakati menghasilkan nilai rata-rata 2,5 menunjukan bahwa sebagian besar proses keamanan informasi telah diterapkan secara konsisten karena semua pihak yang terlibat telah menyadari tanggungjawab masing masing dalam pengamanan informasi.

5. SARAN

Berikut merupakan hal-hal yang dapat dilakukan untuk melakukan penelitian selanjutnya:

a. Telah disusun hasil audit keamanan sisitem informasi pada PT. Suara Merdeka Press dimana harus segera menerapkan kebijakan-kebijakan dan prosedur untuk mengatasi kelemahan atau kekurangan yang ditemukan.
b. Perlunya diadakan pelatihan untuk staff yang berkopeten pada bidangnya agar sumber daya manusia pada PT. Suara Merdeka Press bias mengikuti perubahan.
c. Audit keamanan sistem informasi ini masih belum menerapkan seluruh kontrol keamanan yang telah dipetakan di karenakan keterbatasan auditor untuk mengakses data perusahaan. Sehingga diharapkan setelah seluruh sistem perusahaan telah berjalan sesuai dengam proses bisnis yang ada atau setelah membuat prosedur sistem manajemen keamanan informasi yang baru maka perlu dilakukan audit keamanan sistem informasi kembali untuk menentukan maturity level yang baru setelah perusahaan sudah melakukan perbaikan pada sistem keamanan informasinya.
d. PT. Suara Merdeka Press harus melakukan audit secara berkala untuk mengurangi risiko pada keamanan informasi setidaknya setahun sekali.

UCAPAN TERIMA KASIH

Penulis mengucapkan teima kasih kepada Universitas Dian Nuswantoro, Rektor UDINUS, Dekan Fakultas Ilmu Komputer, Kaprodi Sistem Informasi-S1, Dosen pembimbing, Dosen-dosen pengampu kuliah di Fakultas Ilmu Komputer, serta teman-teman dan sahabat yang selama ini telah mendampingi penulis selama kuliah di Universitas Dian Nuswantoro.

DAFTAR PUSTAKA

[1] Lussianty,dkk 2013 "*Pengukuran Risiko Informasi Teknologi Pada PT. Street Directory Indonesia dengan Menggunakan ISO/IEC 27001/2"* Jakarta: Universitas Bina Nusantara.

[2] Arbi Kusuma, dkk 2014 *"Audit Keamanan Sistem Informasi Berdasarkan Standar SNI-ISO 27001 Pada Sistem Informasi Akademik Universitas Islam Negeri Sunan Kalijaga Yogyakarta"* Yogyakarta: UIN Sunan Kalijaga.

[3] Rainer & Cegielski, "*Introduction to Information Systems: Enabling and Transforming Business*", *2013.*

[4] Thomas R. Peltier, *"Information Security Risk Analysis, Second Edition", 2005*

[5] Alan Calder, Steve Watkins, *"IT Governance: An International Guide to Data Security and ISO27001/ISO27002", 2012*

[6] Syafrizal, Melvin. 2008. *Information Security Management System (ISMS) Menggunakan ISO/IEC 27001:2005* Yogyakarta

[7] Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik. 2011

[8] ISO/IEC 27001:2005, *Information Technology – Security Techniques -- Information security management systems – Requirements*

[9] Reza Zulfikar Ruslam, dkk 2013 "*Audit Kepatuhan Keamanan Informasi Dengan Menggunakan Framework ISO 27001/ISMS"* Jakarta : Universitas Indonesia

[10] Direktorat Badan Standarisasi Nasional, 2009. SNI ISO/IEC 27001:2009 *Teknologi Informasi-Teknik Keamanan-Sistem Manajemen Keamanan Informasi-Persyaratan*. Jakarta: Badan Standarisasi Nasional.