AUDIT KEAMANAN INFORMASI PADA BAGIAN PENGEMBANGAN MULTIMEDIA BARU BERDASARKAN STANDAR ISO 27002:2005 DI RADIO REPUBLIK INDONESIA SURABAYA

Dewangga Putra Sejati[1)] **Haryanto Tanuwijaya**[2)] **Erwin Sutomo**[3)]
Program Studi/Jurusan Sistem Informasi
Institut Bisnis dan Informatika Stikom Surabaya, Sistem Informasi
Jl. Raya Kedung Baruk 98 Surabaya, 60298
Email : 1)dewanggaputra90@yahoo.co.id, 2)haryanto@stikom.edu, 3)sutomo@stikom.edu

Abstract: *Pengembangan Media Baru (PMB) is part of information management data used to support the broadcast, such as : save the news will be broadcast, save songs, supporting tasks broadcast in the scope of Radio RRI Surabaya. PMB also collect temporary news from all third class station in East Java and then sent it to first class station at a certain time span. So far, PMB had Confidentiality problems is saving news error that doesn't match with the planning. The impact of this problem is disruption of the broadcaster to read the news, so that live broadcast become inaccurate. From integrity side is the wholeness of the news coverage results directly accessed was incomplete. The woleness of the news coverage of incomplete results will have an impact on the fall of broadcast event rating and influencing the quality of that event. From availability side, is the delay of provision of information, news, live events, entertainment, and advertising. It can lead to the risk of decrease trust level from listeners and stakeholders RRI Surabaya, and causing losses for RRI Surabaya.*

Referring to the results of the reviews, surveys, and interviews that have been done, so standard ISO 27002: 2005 is selected. There are three clause assigned is human resources security (Clause 8), the secure area (Clause 9), access control (Clause 11).The result of the calculation process maturity level of audit information security on the PMB RRI Surabaya is 2.55 which is managed. That results showed the most of information security process at PMB RRI Surabaya is still in the development stage with limited documentation.

Keywords*: Audit, Information Security, ISO27002:2005, level of maturity.*

RRI Surabaya ialah instansi yang mengadakan penyiaran dalam bentuk berita dan tayangan sosial diantaranya adalah lagu, berita serta siaran lainya. Berbagai acara yang telah disebutkan secara umum disiarkan guna mencukupi keperluan pendengar tentang berita dan hiburan agar pendengar dapat mengetahui kejadian yang ada di seluruh dunia secara langsung. Maka dari itu dalam melaksanakan siaran ini, RRI memiliki visi untuk pedoman. Visi tersebut diantaranya ialah: Menyiarkan berita pemerintahan, memutar tayangan sosial seperti, lagu, sandiwara untuk pendengar, dan mengajarkan tentang pendidikan.

Mengacu Surat MENKOMINFO No.03/PER/M.KOMINFO/03/2011 tanggal 16 Maret 2011, RRI Surabaya menempati stasiun kelas dua yang beralamatkan di Jl. Pemuda No. 82-90 Surabaya. RRI Surabaya memiliki beberapa aset diantaranya aset informasi, piranti lunak, fisik, dan layanan. Salah satu aset diatas dikelola pada bagian Pengembangan Multimedia Baru (PMB) yang merupakan bagian pengelolaan informasi data yang digunakan untuk menunjang siaran seperti: menyimpan berita yang akan disiarkan, menyimpan lagu, serta tugas yang mendukung siaran dalam lingkup Radio RRI Surabaya. Bagian PMB juga mengumpulkan sementara berita dari seluruh stasiun kelas tiga Jawa Timur yang selanjutnya dikirim ke stasiun kalas satu pada rentang waktu tertentu.

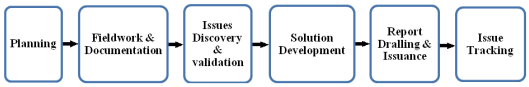
Bagian PMB yang dimiliki oleh RRI Surabaya terintegrasi dengan seluruh RRI kelas tiga seluruh Tawa Timur dan RRI kelas satu di Jakarta. Selain itu RRI Surabaya terintegrasi secara online dan memiliki jaringan komputer yang terbagi menjadi empat server, yaitu server berita, lagu, backup, dan server streaming. Dengan demikian, sebagai stasiun penyiaran kelas dua yang memiliki seluruh informasi penyiaran publik RRI Surabaya harus memiliki

jaringan streaming data, back up, dan recovery yang berjalan dengan baik.

Selama ini bagian PMB mengalami permasalahan dari sisi *Confidentiality* adalah kesalahan penyimpanan berita yang tidak sesuai dengan perencanaan. Dampak dari permasalahan ini adalah terganggunya pihak penyiar membaca berita, sehingga siaran langsung menjadi tidak akurat. Dari sisi *Integrity* adalah keutuhan berita hasil liputan langsung yang diakses tidak lengkap. Keutuhan berita hasil liputan yang tidak lengkap akan berdampak pada turunya rating acara siaran serta mempengaruhi kualitas acara tersebut. Dari sisi *Availability* adalah keterlambatan peyediaan informasi, berita, siaran langsung, hiburan, dan iklan. Hal ini dapat menyebabkan terjadinya risiko menurunya tingkat kepercayaan pendengar dan *stakeholder* pada RRI Surabaya, serta menyebabkan kerugian bagi RRI Surabaya. Selama ini bagian PMB belum pernah melakukan analisa akibat permasalahan tersebut, atas kejadian tersebut bagian PMB belum mengetahui tingkat keamanan yang dimiliknya.

Pemilihan *standard* ISO 27002:2005 digunakan sebagai acuan karena didalamnya berisi panduan praktis mengenai tehnik keamanan informasi. Selain itu *standard* ISO 27002:2005 juga memiliki dokumen SMKI. *Standard* ini tidak mengkhususkan bentuk kontrol yang tertentu tetapi menyerahkan kepada pengguna untuk memilih dan menerapkan kontrol yang tepat sesuai kebutuhannya khususnya pada bagian PMB.

METODE PENELITIAN



Gambar 1. Tahapan dalam Audit Keamanan Informasi
(Sumber: Davis, 2011)

Dari 6 metode tahapan (Davis,2011) dari 6 tahapan dalam gambar 1 penulis menggunakan 4 metode sebagai acuan tahapan yaitu:

1. Perencanaan audit dengan menghasilkan dokumen profil instansi, visi misi instansi, struktur organisasi, deskripsi pekerjaan, proses kerja, ruang lingkup obyek audit dan tujuan audit, hasil pemilihan klaosul, kontrol dan obyektif kontrol, serta *engagement letter*.
2. Presiapan audit dengan hasil keluaran hasil penyusunan AWP/ rencana kerja, hasil penyampaian kebutuhan data, hasil pernyataan, hasil pembobotan, serta daftar pertanyaan audit.
3. Hasil pelaksanaan audit dengan hasil keluaran dokumen hasil wawancara, dokumen hasil pemeriksaan data, hasil uji kematangan, dan daftar temuan dan rekomendasi.
4. Pelaporan audit dengan hasil keluaran hasil daftar temuan audit dan rekomendasi, pertemuan penutup, notulen pertemuan penutup.

HASIL DAN PEMBAHASAN

Pemahaman Proses Bisnis TI

Dalam tahap perencanaan, pemahaman proses bisnis dan TI adalah hal yang pertama yang harus dilakukan oleh seorang auditor untuk mengetahui seluk beluk instansi penyiaran sebelum dilakukan audit dengan cara memahami dokumen instansi penyiaran, seperti profil instansi penyiaran, rencana jangka pendek dan rencana jangka panjang di Radio Republik Indonesia (RRI) Surabaya, profil Pengembangan Multimedia Baru (PMB) RRI Surabaya, struktur organisasi fungsional PMB. Tugas pokok dan fungsi (TUPOKSI) pegawai PMB RRI Surabaya, proses bisnis PMB RRI Surabaya.

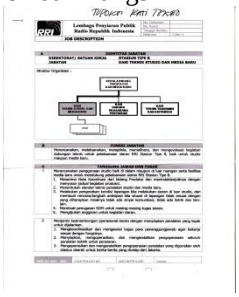
1. Visi RRI Surabaya:
   Radio Republik Indonesia sebagai lembaga penyiaran pubik yang independen, netral, mandiri dan profesional.
2. Misi RRI Surabaya:
   a) Mendukung terwujudnya kerjasama dan saling pengertian dengan negara-negara sahabat khususnya dan dunia internasional pada umumnya.
   b) Ikut mencerdaskan kehidupan bangsa dan mendorong terwujudnya masyarakat informasi.
   c) Meningkatkan kesadaran bermasyarakat, berbangsa dan bernegara yang demokratis dan berkeadilan, serta menjunjung tinggi supremasi hukum dan hak asasi manusia.
   d) Merekatkan persatuan dan kesatuan bangsa.
   e) Melaksanakan kontrol sosial.
   f) Mengembangkan jati diri dan budaya bangsa.
3. Profil Pengembangan Multimedia Baru (PMB) pada RRI Surabaya

Pengembangan Multimedia Baru (PMB) merupakan bagian dari teknik studio dan media baru instansi penyiaran radio RRI Surabaya, sedangkan teknik studio dan multimedia baru merupakan unit dari stasuin penyiaran RRI Surabaya. PMB adalah bagian yang mendukung fasilitas dan kebutuhan penyiaran RRI wilayah Jawa Timur. Beberapa kebutuhan di bagian penyiaran yaitu penyimpanan, pengelolaan berita, lagu, siaran, iklan, streaming, dan lain-lain untuk stasiun penyiaran kelas II (dua) RRI Surabaya.

4. Struktur Organisasi Fungsional di PMB

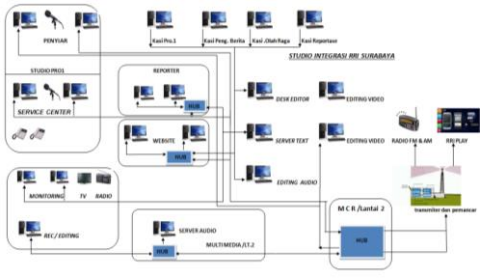
Gambar 2. Struktur Organisasi PMB

5. Tugas pokok dan Fungsi PMB



Gambar 3. Tugas Pokok dan Fungsi Kepala Seksi PMB

6. Diagram Studio Integrasi



Gambar 4. Diagram Studio Integrasi

Penentuan Ruang Lingkup, Obyek dan Tujuan Audit

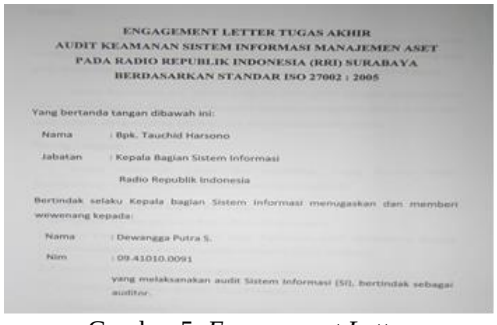
Dalam melakukan penelitian audit keamanan sistem informasi, digunakan *standard* ISO 27002:2005 dan dengan 3 klausul sebagai acuan dalam pelaksanaan audit terdapat pada Tabel 2. Adapun dalam menetapkan klausul, obyektif kontrol dan kontrol yang sesuai berdasarkan permasalahan dilapangan serta kesepakatan bersama kedua belah pihak. Sehingga hasil yang didapatkan adalah klausul 8 (Keamanan Sumber Daya Manusia), Klausul 9 (Keamanan Fisik dan Lingkungan) dan Klausul 11 (Kontrol Akses). Penentuan ruang lingkup dilakukan dengan cara melakukan observasi pada bagian PMB.

Tabel 1. Pemetaan Ruang Lingkup dan Klausul

No	Klausul	Objektif/Kontrol	Kontrol
1.	Klausul 8 Keamanan Sumber Daya Manusia	a. 8.1 Sebelum Menjadi Pegawai b. 8.2 Selama Menjadi Pegawai c. 8.3 Pemberhentian atau pemindahan pegawai	a. 8.1.1 Aturan dan tanggung jawab keamanan b. 8.2.1 Tanggung jawab manajemen c. 8.2.2 Pendidikan dan pelatihan keamanan informasi d. 8.3.1 Tanggung jawab pemberhentian
2.	Klausul 9 Keamanan Fisik dan Lingkungan	a. 9.1 Wilayah Aman b. 9.2 Keamanan Peralatan	a. 9.1.2 Kontrol masuk fisik b. 9.1.3 Keamanan kantor, ruang dan fasilitasnya c. 9.2.1 Letak peralatan dan penganamanannya d. 9.2.3 Keamanan pengkabelan
3.	Klausul 11 Kontrol akses	a. 11.1 Persyaratan Bisnis Untuk Akses Kontrol b. 11.2 Manajemen Akses User c. 11.3 Tanggung Jawab Penggguna d. 11.4 Kontrol Akses Jaringan e. 11.5 Kontrol Akses Sistem Operasi f. 11.6 Kontrol Akses Informasi dan Aplikasi g. 11.7 Komputasi Bergerak dan Bekerja Dari Lain Tempat	a. 11.1.1 Kebijakan kontrol akses b. 11.2.3 Manajemen kata sandi penggguna c. 11.2.4 Tinjauan terhadap hak akses user d. 11.3.1 Penggunaan kata sandi e. 11.4.1 Kebijakan penggunaan layanan jaringan f. 11.5.3 Sistem Manajemen kata sandi g. 11.6.1 Pembatasan akses informasi h. 11.7.1 Komunikasi dan terkomputerisasi yang bergerak i. 11.7.2 Teleworking

Engagement Letter

Lampiran *engagement letter* dalam Gambar 5 dibuat oleh auditor agar mendapat persetujuan mengenai kegiatan audit keamanan informasi di bagian PMB, agar *auditee* memberi akses kepada auditor terhadap keamanan informasi dibagian PMB dan lingkunganya. Isi dari *engagement letter* adalah tugas, tujuan, tugas dan tanggung jawab, kewenangan, kode etik, ruang lingkup, waktu pelaksanaan, dan penutup.



ENGAGEMENT LETTER TUGAS AKHIR
AUDIT KEAMANAN SISTEM INFORMASI MANAJEMEN ASET
PADA RADIO REPUBLIK INDONESIA (RRI) SURABAYA
BERDASARKAN STANDAR ISO 27002 : 2005

Yang bertanda tangan dibawah ini:

Nama : Bpk. Tauchid Harsono
Jabatan : Kepala Bagian Sistem Informasi
Radio Republik Indonesia

Bertindak selaku Kepala bagian Sistem Informasi menugaskan dan memberi wewenang kepada:

Nama : Dewangga Putra S.
Nim : 09.41010.0091
yang melaksanakan audit Sistem Informasi (SI), bertindak sebagai auditor.

Gambar 5. *Engagement Letter*

Hasil Pernyataan

Pada hasil pernyataan dihasilkan dari dokumen yang mengacu pada ISO 27002:2005 Klausul 8. Berikut di jelaskan pada Tabel 2 contoh pernyataan klausul 8.

Tabel 2. Hasil Pernyataan

PERNYATAAN AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)	
Klausul 8.1 Sebelum Menjadi Pegawai (*Prior to Employement*)	
ISO 27002 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*)	
Kontrol : Aturan-aturan dan tanggung jawab keamanan dari pegawai, kontraktor dan pengguna pihak ketiga harus didefinisikan, didokumentasikan sesuai dengan kebijakan keamanan informasi organisasi.	
No.	PERNYATAAN
1.	Terdapat peraturan pada proses penerimaan pegawai pada RRI Surabaya
2.	Terdapat prosedur kebijakan tanggung jawab pegawai terhadap perlindungan aset
3.	Terdapat peran dan tanggung jawab dalam melaksanakan dan bertindak sesuai dengan kebijakan keamanan informasi organisasi yang ada
4.	Terdapat kepastian bahwa tanggung jawab pegawai benar benar sudah diberikan demi melindungi keamanan informasi

Hasil Pembobotan

Hasil pembobotan didapatkan dari diskusi antara auditor dan *auditee*, pernyataan tersebut mewakili hasil perhitungan tingkat kematangan bagi instansi. Pada Tabel 3 adalah hasil pembobotan pada klausul 11.

Tabel 3. Hasil Pembobotan

PEMBOBOTAN PERNYATAAN AUDIT KEAMANAN INFORMASI KLAUSUL 11 (KONTROL AKSES)		Auditor : Dewangga Putra Sejati Auditee: Tauchid Harsono NIP. 19651018 198503 1 003 Tanggal: 15 Maret 2016 Tanda tangan:		
PERNYATAAN AUDIT KEAMANAN INFORMASI KLAUSUL 11 (KONTROL AKSES)				
Klausul 11.3 Tanggung Jawab Pengguna (*user*)				
ISO 27002 11.3.1 Penggunaan *password*				
Kontrol : Pengguna seharusnya mengikuti praktek keamanan yang baik dalam pemilihan dan penggunaan kata sandi.				
No.	PERNYATAAN	Bobot		
		Rendah (0,1-0,3)	Sedang (0,4-0,6)	Tinggi (0,7-1,0)
1.	Adanya kesadaran dari diri sendiri untuk menjaga kerahasiaan password			0,7
2.	Terdapat penggantian kata password setiap kali ada kemungkinan sistem atau password dalam keadaan bahaya			0,8
3.	Terdapat larangan dalam pembuatan catatan password			0,7
4.	Terdapat larangan untuk tidak membagi satu password kepada pengguna lain		0,6	
5.	Terdapat pergantian password	0,3		

Daftar Pertanyaan

Beberapa sesi tanya jawab diajukan untuk *auditee* guna mendukung aktivitas audit keamanan informasi. Dimana setiap pertanyaan mengacu pada pernyataan yang telah dibuat sebelumnya. Pada Tabel 4 merupakan hasil pertanyaan klausul 9.

Tabel 4. Daftar Pertanyaan

AUDIT KEAMANAN INFORMASI KLAUSUL 9 (KEAMANAN FISIK & LINGKUNGAN)	
Klausul 9.1 Wilayah Aman (*Secure Areas*)	
ISO 27002 9.1.2 Kontrol masuk fisik	
	P: Apabila ada pengunjung atau selain karyawan masuk ke ruangan server/ PMB, bagaimana syarat khusus untuk pengunjung tersebut? Apa saja yang boleh dilakukan pengunjung yang tidak memiliki pemandu ataupun tanda pengenal tersebut? J: Pengunjung harus memiliki maksud dan tujuan, jika tidak maka tidak akan terlayani oleh PMB.
5	Hak akses ke wilayah aman harus dikaji ulang
	P: Apakah hak akses menuju wilayah aman dilakukan pengkajian ulang secara berkala? J: Tidak pernah, karena hak akses sudah jelas meski tidak tertulis.

Dokumen Hasil Wawancara

Sesi tanya jawab dengan Kepala Seksi PMB yang dilakukan oleh auditor dengan ruang lingkup klausul 9 membahas keamanan fisik dan lingkungan, Staff PMB dengan klausul 8 mengenai Keamanan sumber daya manusia dan klausul 11 tentang Kontrol Akses. Dalam Tabel 5 merupakan hasil tanya jawab pada klausul 9.

Tabel 5. Hasil Wawancara

PROGRAM PEMERIKSAAN AUDIT KEAMANAN INFORMASI ASPEK : KLAUSUL 9 (KEAMANAN FISIK & LINGKUNGAN)		Pemeriksa : Dr. Haryanto Tanuwijaya, S.Kom., M.MT. Auditor : Dewangga Putra Sejati Auditee : Tauchid Harsono, SPt. Tanggal : 22 Maret – 09 April 2016 Tanda Tangan :	
Klausul 9.1 Wilayah Aman (*Secure Area*)			
ISO 27002 9.1.2 Kontrol masuk fisik			
No.	Pemeriksaan	Catatan Auditor	Catatan Review
		urusan atau berkepentingan dengan staf pegawai maupun keperluan dengan kepala seksi PMB dan diawasi dengan CCTV.	
2.	Identifikasi orang yang memasuki wilayah aman hanya diberikan akses untuk tujuan dan otorisasi tertentu Dengan cara: 1. Wawancara.. 2. Survey.	Telah diperiksa bahwa selain karyawan hanya diperbolehkan melakukan kegiatan yang berkaitan dengan urusan pengajaran dan diawasi kepentinganya oleh karyawan. Anabila ada orang-	Selain pegawai di perbolehkan melakukan kegiatan sebatas pengajaran dan adapun sanksi bagi orang selain pegawai yang melakukan suatu hal yang mengganggu proses kerja.

Dokumen Hasil Pemeriksaan Data

Dalam pelaksanaan pemeriksaan data yang ada dalam program audit telah dilaksanakan oleh auditor dengan menggunakan teknik audit yang sesuai serta melampirkan bukti pendukung secara tepat. Dalam Tabel 6 memberikan hasil pemeriksaan data pada klausul 8 keamanan sumber daya manusia.

Tabel 6. Dokumen Pemeriksaan data

PROGRAM PEMERIKSAAN AUDIT KEAMANAN INFORMASI ASPEK : KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)		Pemeriksa : Dr. Haryanto Tanuwijaya, S.Kom., M.MT. Auditor : Dewangga Putra Sejati Auditee : Gilang Satio Nugroho Tanggal : 22 Maret – 09 April 2016 Tanda Tangan :	
Klausul 8.1 Sebelum Menjadi Pegawai (*Prior to Employement*)			
ISO 27002 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*)			
No.	Pemeriksaan	Catatan Auditor	Catatan Review
1.	Identifikasi peraturan pada proses penerimaan pegawai Dengan cara: 1. Wawancara. untuk proses penerimaan pegawai 2. Didapatkan keterangan mengenai peraturan pada proses penerimaan pegawai.	Telah dilakukan pemeriksaan bahwa terdapat peraturan khusus pada proses penerimaan pegawai di RRI Sby.	Telah terdapat peraturan khusus penerimaan PNS, di dinas RRI Surabaya serta terdapat pula surat keputusan pengangkatan PNS di RRI Sby. Lampiran: foto surat keputusan.
2.	Identifikasi prosedur kebijakan mengenai tanggung jawab pegawai terhadap perlindungan aset	Telah diperiksa bahwa dilakukan perlindungan aset oleh bagian PMB. Dan dokumentasinya	Terdapat dokumen tanggung jawab pegawai dalam melindungi aset oleh bagian PMB.

Hasil Uji Kematangan

Untuk mengetahui tingkat kematangan pada penerapan pengamanan pada uji kematangan dengan memakai perhitungan dari (CMMI) *Capability Maturity Model for Integration* to ISO 27002 terdapat pada Tabel 7. Berdasarkan analisa dari hasil tanya jawab dengan *auditee*, pengumpulan bukti, dan, pemeriksaan. Hasil uji kepatutan diperoleh dari perhitungan tingkat kematangan masing-masing kontrol, hasil perhitungan tingkat kematangan pada klausul 8 terdapat pada tabel 7. Pada tabel 8 adalah, pada gambar 6 adalah representasi tingkat nilai kematangan. Hasil uji kematangan ini dapat menjadi keterangan menunjukkan keadaan keamanan informasi bagian PMB pada saat ini.

Tabel 7. Representasi CMMI to ISO 27002

Level	*Continous Representation Capability Levels*	*Staged Representation Maturity Levels*
0	***Incomplete***	
1	***Performed***	***Initial***
2	***Managed***	***Managed***
3	***Defined***	***Defined***
4		***Quantitatively Managed***
5		***Optimizing***

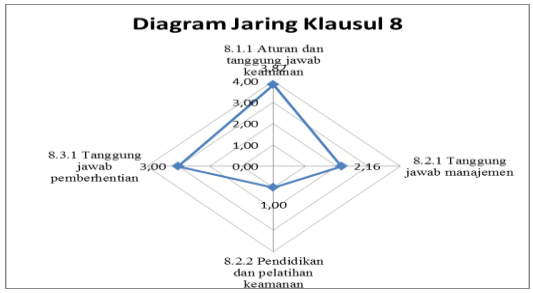
(Sumber: CMMI-DEV V1.3, 2010)

Tabel 8. Hasil Tingkat Kematangan klausul 8

Klausul 8 (keamanan sumber daya manusia)										
Klausul 8.1 Sebelum Menjadi Pegawai (*Prior to Employement*)										
ISO 27002 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*)				Tingkat kematangan						Nilai
				0	1	2	3	4	5	
No	Pernyataan	Hasil Pemeriksaan	Bobot	Non-existent	Initial	Repeatable	Defined	Managed	Optimized	
1.	Terdapat peraturan pada proses penerimaan pegawai pada RRI Sby	Telah terdapat peraturan khusus penerimaan PNS, di dinas RRI Surabaya serta terdapat pula surat keputusan pengangkatan PNS di RRI Sby. Lampiran: foto surat keputusan.	0,3					√		1,2
2.	Terdapat prosedur kebijakan tanggung jawab pegawai terhadap perlindungan aset	Terdapat dokumen tanggung jawab pegawai dalam melindungi aset oleh bagian PMB. Lampiran: SKP Basuki	0,3				√			0,9
3.	Terdapat peran dan tanggung jawab dalam melaksanakan dan bertindak sesuai dengan kebijakan keamanan informasi organisasi yang ada	Peran dan tanggung jawab pegawai di bagian PMB sudah tertuang dalam dokumen TUPOKSI tentang tanggung jawab yang dimiliki masing masing pihak seperti pegawai PNS, dan pegawai non PNS. Lampiran: foto TUPOKSI PNS dan	0,6					√		2,4
4.	Terdapat kepastian bahwa tanggung jawab pegawai benar benar sudah diberikan demi melindungi keamanan informasi	Dokumentasi tentang kepastian tanggung jawab pegawai dalam melindungi keamanan informasi tertuang dalam LCK pegawai masing-masing. Lampiran: Dokumen SKP.	0,5					√		2
Total bobot			1,7	Tingkat Kematangan		3,82		Total nilai		6,5

Tabel 9. Hasil Perhitungan Tingkat kematangan klausul 8

Klausul	Obyektif Kontrol	Kontrol keamanan	Tingkat Kemampuan	Rata-rata obyektif kontrol
8 Keamanan sumber daya manusia	8.1 Sebelum Menjadi Pegawai	8.1.1 Aturan dan tanggung jawab keamanan	3,82	3,82
	8.2 Selama Menjadi Pegawai	8.2.1 Tanggung jawab manajemen	2,16	1,58
		8.2.2 Pendidikan dan pelatihan keamanan informasi	1,00	
	8.3 Pemberhentian atau pemindahan pegawai	8.3.1 Tanggung jawab pemberhentian	3,00	3,00
Maturity Level Klausul 8				2,80

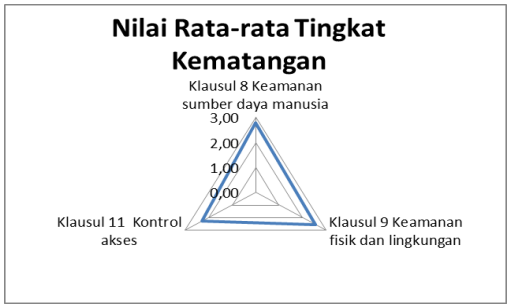


Gambar 6. Representasi Nilai Tingkat Kematangan Klausul 8

Dari proses perhitungan didapat nilai tingkat kematangan pada klausul 8 adalah (2,80) yaitu *managed*. Hal ini menunjukan bahwa proses keamanan sumber daya manusia masih sedikit. Hasil perhitungan tingkat kematangan semua klausul terdapat pada Tabel 10, dan hasil representasi tingkat kematangan seluruh klausul ada pada gambar 7.

Tabel 10. Hasil Rata-Rata Tingkat Kematangan Semua Klausul

Klausul	Deskripsi	Tingkat Kematangan
8	Keamanan sumber daya manusia	2,80
9	Keamanan fisik dan lingkungan	2,54
11	Kontrol akses	2,30
Nilai rata-rata Tingkat kematangan		2,55



Gambar 7. Hasil Representasi *Maturity Level* Semua Klausul

Hasil perhitungan *maturity level* audit keamanan informasi pada bagian PMB RRI Surabaya adalah 2,55 yakni *managed*. Hasil tersebut menunjukan kalau beberapapa bagian

besar dari proses keamanan informasi pada bagian Pengembangan Media Baru Radio Republik Indonesia Surabaya masih dikembangkan dengan keterbatasan dokumentasi dari instansi.

Daftar Temuan dan Rekomendasi

Auditor memberikan hasil Rekomendasi berdasarkan hasil temuan dan penentuan nilai dari bobot rendah (0,1-0,3), sedang (0,4-0,6), dan tinggi (0,7-1,0) telah diberikan oleh auditor untuk *auditee*. Hasil temuan dan rekomendasi klausul 8 terdapat pada Tabel 11, dan pada Gambar 8 merupakan temuan surat keputusan.

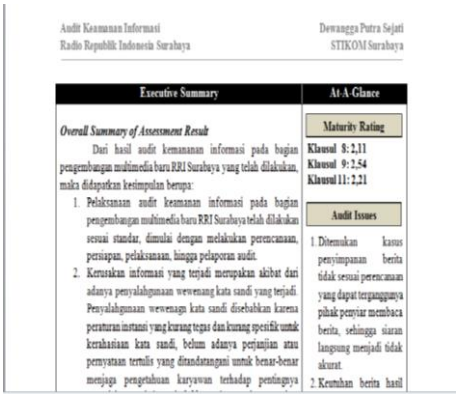
Tabel 11. Hasil Temuan dan Rekomendasi

PROGRAM PEMERIKSAAN AUDIT KEAMANAN INFORMASI ASPEK : KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)		Pemeriksa : Dr. Haryanto Tanuwijaya, S.Kom., M.MT. Auditor : Dewangga Putra Sejati Auditee : Gilang Setio Nugroho Tanggal : 22 Maret – 09 April 2016 Tanda Tangan :	
Klausul 8.1 Sebelum Menjadi Pegawai (*Prior to Employement*) ISO 27002 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*)			
No.	Pemeriksaan	Catatan Auditor	Catatan Review
1.	Identifikasi peraturan pada proses penerimaan pegawai Dengan cara: 1. Wawancara, untuk proses penerimaan pegawai 2. Didapatkan keterangan mengenai peraturan pada proses penerimaan pegawai	Telah dilakukan pemeriksaan bahwa terdapat peraturan khusus pada proses penerimaan pegawai di RRI Sby.	Telah terdapat peraturan khusus penerimaan PNS, di dinas RRI Surabaya serta terdapat pula surat keputusan pengangkatan PNS di RRI Sby. Lampiran: foto surat keputusan.
2.	Identifikasi prosedur kebijakan mengenai tanggung jawab pegawai terhadap perlindungan aset	Telah diperikasa bahwa dilakukan perlindungan aset oleh bagian PMB. Dan dokumentasinya	Terdapat dokumen tanggung jawab pegawai dalam melindungi aset oleh bagian PMB

Gambar 8. Surat keputusan

Hasil Pelaporan Audit

Setelah dilakukan pelaksanaan audit keamanan sistem informasi auditor wajib memberikan laporan kepada *auditee*. Laporan audit hanya ditunjukan kepada pihak yang berhak saja, karena bersifat rahasia. Berikut contoh pelaporan audit gambar 9.



Audit Keamanan Informasi — Dewangga Putra Sejati
Radio Republik Indonesia Surabaya — STIKOM Surabaya

Executive Summary

Overall Summary of Assessment Result

Dari hasil audit kemanan informasi pada bagian pengembangan multimedia baru RRI Surabaya yang telah dilakukan, maka didapatkan kesimpulan berupa:

1. Pelaksanaan audit keamanan informasi pada bagian pengembangan multimedia baru RRI Surabaya telah dilakukan sesuai standar, dimulai dengan melakukan perencanaan, persiapan, pelaksanaan, hingga pelaporan audit.
2. Kerusakan informasi yang terjadi merupakan akibat dari adanya penyalahgunaan wewenang kata sandi yang terjadi Penyalahgunaan wewenagn kata sandi disebabkan karena peraturan instansi yang kurang tegas dan kurang spesifik untuk kerahasiaan kata sandi, belum adanya perjanjian atau pernyataan tertulis yang ditandatangani untuk benar-benar menjaga pengetahuan karyawan terhadap pentingnya

At-A-Glance

Maturity Rating

Klausul 8: 2,11
Klausul 9: 2,54
Klausul 11: 2,21

Audit Issues

1. Ditemukan kasus penyimpanan berita tidak sesuai perencanaan yang dapat terganggunya pihak penyiar membaca berita, sehingga siaran langsung menjadi tidak akurat.
2. Keamhan berita hasil

Gambar 9. Hasil Pelaporan Audit

SARAN

Dari semua runtutan audit yang telah dilakukan maka saran dapat diberikan kepada instansi demi pengembangan lebih baik dalam waktu yang akan datang adalah:

1. Pada bagian PMB RRI Surabaya setidaknya satu tahun sekali wajib melakukan audit keamanan informasi secara berkelanjutan untuk menanggulangi risiko gangguan keamanan informasi.
2. Bagian PMB dalam audit keamanan informasi. Beberapa klausul standar ISO 27002:2005 dapat diterapkan dalam audit keamanan informasi RRI Surabaya pada kesempatan lain.

RUJUKAN

Davis dkk. 2011. *IT Auditting: Using Controls to Protect Information Assets Second Edition.* United States: The McGraw-Hill Companies.

ISO/IEC 27002. 2005. *Information technology — Security techniques — Code of practice for information security management International.*ISO.

P. Menteri Komunikasi dan Informatika No. 03/PER/M.KOMINFO/03/2011 Tentang Organisasi dan Tata Kerja Unit Pelaksana Teknis Bidang Monitor Spektrum Frekuensi Radio.

Sarno, R. dan Iffano, I. 2009. *Sistem Manajemen Keamanan Informasi*. Surabaya: ITS Press.

Sarno, Riyanarto. 2009. *Audit Sistem & Teknologi Informasi*. Surabaya: ITS Press.

Tanuwijaya, H. dan Sarno, R. 2010. *Comparation of Cobit Maturity Model and Structural Equation Model for Measuring the Aligment beetween University Academic Regulations and Information Technology Goals*, International Journal of Computer Science and Network Security, VOL.10 No.6, June 2010.