BAB IV

HASIL DAN PEMBAHASAN

Pada bab ini akan diuraikan tentang hasil dan pembahasan bab III dari tahap perencanaan audit keamanan informasi yaitu tahap persiapan audit keamanan sistem informasi, tahap pelaksanaan audit keamanan sistem informasi, serta tahap pelaporan audit keamanan informasi.

4.1 Hasil Tahap Perencanaan Audit Keamanan Informasi

Hasil dari tahapan perencanaan ini berupa: 1. Profil perusahaan, visi, misi Radio Republik Indonesia (RRI) Surabaya, profil Pengembangan Multimedia Baru (PMB), struktur organisasi, deskripsi pekerjaan di bagian PMB, dan proses kerja, 2. Ruang lingkup, obyek audit dan tujuan audit, 3. Hasil pemilihan klausul, obyektif kontrol dan kontrol, 4. Hasil perjanjian audit berupa surat perjanjian audit atau *Engagement Letter*.

4.1.1 Hasil Pemahaman Proses Bisnis dan TI

Pada perencanaan audit, pemahaman proses bisnis dan TI merupakan hal yang pertama yang harus dilakukan oleh seorang auditor untuk mengetahui seluk beluk instansi penyiaran sebelum dilakukan audit dengan cara memahami dokumen instansi penyiaran, yaitu profil instansi penyiaran, visi dan misi RRI Surabaya, profil PMB RRI Surabaya, struktur organisasi fungsional PMB. Tugas pokok dan fungsi (TUPOKSI) pegawai PMB RRI Surabaya, proses bisnis PMB RRI Surabaya.

1. Profil RRI Surabaya

Republik Indonesia merupakan Lembaga Penyiaran Publik milik bangsa Indonesia didirikan pada tanggal 11 September 1945. Radio Republik Indonesia sampai tahun 2009 memiliki 59 stasiun penyiaran tersebar di seluruh Indonesia serta ditambah 1 stasiun penyiaran Siaran Luar Negeri yang dikenal dengan *Voice Of Indonesia*. Pada sebuah stasiun penyiaran RRI di kota besar biasanya terdapat 4 programa antara lain PRO1, PRO2, PRO3 dan PRO4. Segmentasi PRO1 Ragam Musik dan Informasi, PRO2 Gaya Hidup, PRO3 Jaringan Berita Nasional, PRO4 Pendidikan dan Budaya, sedangkan Voice Of Indonesia siaran luar negeri yang coverage areanya mencakup Eropa, Timur Tengah, Afrika, Asia Pasifik, Australia, dan Amerika.

2. Visi, Misi dan Tujuan Radio Republik Indonesia

Visi:

Radio Republik Indonesia sebagai lembaga penyiaran pubik yang independen, netral, mandiri dan profesional.

Misi:

1. Mendukung terwujudnya kerjasama dan saling pengertian dengan negara-negara sahabat khususnya dan dunia internasional pada umumnya.
2. Ikut mencerdaskan kehidupan bangsa dan mendorong terwujudnya masyarakat informasi.
3. Meningkatkan kesadaran bermasyarakat, berbangsa dan bernegara yang demokratis dan berkeadilan, serta menjunjung tinggi supremasi hukum dan hak asasi manusia.
4. Merekatkan persatuan dan kesatuan bangsa.

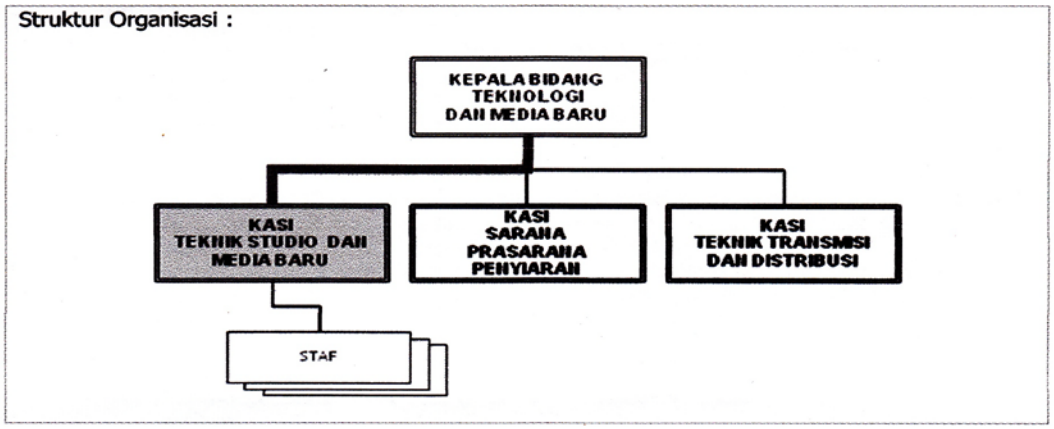
5. Melaksanakan kontrol sosial.
6. Mengembangkan jati diri dan budaya bangsa.

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.

Selama ini bagian PMB belum pernah melakukan analisa penyebab terjadinya permasalahan tersebut, oleh karena itu bagian PMB tidak mengetahui bagaimana tingkat keamanan informasi yang dimiliknya. Evaluasi keamanan informasi dapat dilakukan dengan audit keamanan informasi Hal ini diperlukan untuk memenuhi Surat Perintah Perusahaan RRI Surabaya Nomor: 18/SPI/02/2014 tentang kebijakan keamanan informasi.

4. Struktur Organisasi Fungsional di Pengembangan Multimedia Baru



Gambar 4.1 Struktur Organisasi Pengambangan Multimedia Baru di RRI Surabaya

Gambar 4.1 adalah gambaran struktur organisasi fungsional PMB di RRI Surabaya. PMB memiliki struktur organisasi fungsional yang didalamnya terdapat karyawan yang sesuai pada bidangnya masing-masing. Pada PMB terdapat 5 bagian yang masing-masing bagiannya memiliki *Job Description*.

5. Deskripsi Pekerjaan di PMB

Pengembangan multimedia baru (PMB) mempunyai struktur organisasi fungsionalitas dimana pada stuktur didalamnya terdapat keahlian pekerjaan apa saja yang dimiliki oleh setiap bagiannya. Pada Tabel 4.1 menjelaskan tugas pokok dan fungsi (tupoksi) di bagian PMB.

Tabel 4.1 Tugas Pokok dan Fungsi bagian PMB di RRI Surabaya

No.	Nama & Jabatan / NIP	Deskripsi Tugas
1	**TAUCHID HARSONO & KEPALA SEKSI TEKNIK STUDIO DAN MEDIA BARU / 196510181985031003**	1. Merencanakan penggunaan studio baik di dalam maupun diluar ruangan serta fasilitas media baru untuk mendukung pelaksanaan siaran RRI Stasiun Tipe B. 2. Menjamin kesinambungan operasionalsiaran dengan menyiapkan peralatan yang layak untuk dijalankan. 3. Memonitor pelaksanaan siaran di RRI Stasuin Tipe B khususnya dalam hal dukungan teknis. 4. Melakukan evaluasi pelaksaan dukungan teknis secara berkala. 5. Memelihara peralatan studio dan peralatan untuk luar studio serta fasilitas media baru. 6. Bertanggung jawab terhadap jaringan *website* dan *streaming* media baru. 7. Melakukan fungsi pembinaan bawahan.

Tabel 4.1 (Lanjutan)

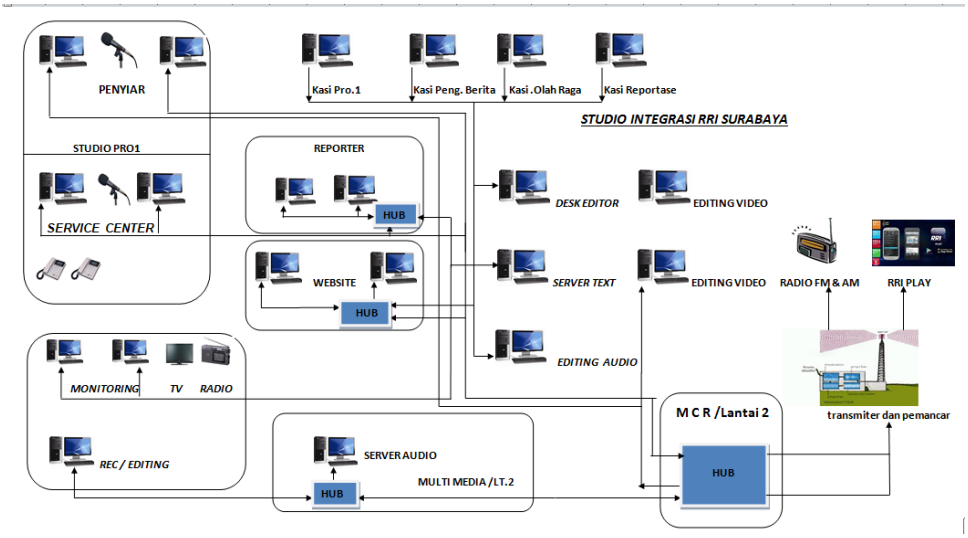
No.	Nama & Jabatan / NIP	Deskripsi Tugas
2	**GIRANG BASUKI, SE. & STAFF TEKNIK STUDIO DAN MEDIA BARU / 197008101994121 001**	1. Melakukan konfigurasi PC secara berkala. 2. Melakukan instalasi dan memelihara security di setiap PC Client. 3. Melakukan instalasi dan operating systemnya. 4. Mengelola Local Area Network. 5. Melakukan instalasi dan maintenance hotspot. 6. Melakukan mintenance web jaringan, web streaming, web server. 7. Membantu user dlm menghadapi masalah hardware, software computer, LAN, dan *audio streaming.* 8. Melakukan maintenance seluruh peralatan multimedia dan melakukan update anti virus.
3	**GILANG SETIO NUGROHO & STAFF TEKNIK STUDIO DAN MEDIA BARU / 19890522 201301 NO1**	1. Melakukan konfigurasi PC secara berkala. 2. Melakukan instalasi dan memelihara security di setiap PC Client. 3. Melakukan instalasi dan operating systemnya. 4. Mengelola Local Area Network. 5. Melakukan instalasi dan maintenance hotspot. 6. Melakukan mintenance web jaringan, web streaming, web server. 7. Membantu user dlm menghadapi masalah hardware, software computer, LAN, dan *audio streaming.* 8. Melakukan maintenance seluruh peralatan multimedia dan melakukan update anti virus.

(Sumber: Bagian PMB RRI Surabaya)

6. Proses bisnis dan TI di bagian pengembangan multimedia baru

   Proses bisnis pada bagian PMB secara garis besar yaitu: reporter melakukan *input* berita dari lapangan dan bagian *monitoring* mendapatkan berita dari beberapa reporter dari RRI kelas tiga, menulis berita dari televisi, radio lain, bagian rec/editing lalu menginputkan ke *server text*. Dibagian *server text* ada *desk editor* dan *editing audio* masing-masing memiliki peran memperbaiki dan evaluasi oleh kasi Pro 1, kasi pengolahan berita, kasi olah raga, kasi reportase. Setelah berita *text* dan *audio* disetujui para kasi maka akan disimpan ke *server audio multimedia* / lantai 2 yang nantinya akan dibaca oleh penyiar studio Pro 1. Pada bagian *website* bertugas mengisi konten berita ke *website* dibagian *editing video* mengambil berita *voice* ke *server audio* agar menghasilkan berita *video*. Pada bagian *server audio* menampung dari *editing / rec* yang disambungkan oleh *hub* ke MCR (Multi Control Room) yang selanjutnya diakses bagian lain. Dalam proses siaran ini semua informasi dalam server *audio multimedia* dapat diakses semua bagian studio Pro1, *service center*, *rec/editing* yang tingkatan kata sandi hanya terdapat pada *login* awal saja, jadi apabila terdapat salah satu karyawan saling menitipkan kata sandi maka akan berisiko merusak informasi berita dan audio. Apabila informasi berita dan audio rusak, masalah yang ditimbulkan yaitu terhambatnya siaran berita pada Pro 1 yang mengakibatkan terlambatnya jadwal siaran, denda dari *stakeholder*, dan menurunya tingkat kepercayaan masyarakat terhadap RRI.

   Berikut adalah alur proses distribusi informasi pada bagian multimedia baru.



Gambar 4.2 Proses Bisnis dan Siaran RRI Surabaya
(Sumber : Dokumen Studio Integrasi RRI Surabaya)

4.1.2 Ruang Lingkup, Risiko audit dan Tujuan Audit

1. Tujuan Audit Keamanan Informasi PMB RRI Surabaya

Tujuan dilakukannya audit keamanan informasi PMB RRI Surabaya adalah untuk mengukur tingkat keamanan informasi yang ada, sehingga dapat menentukan apakah Sistem Manajemen Keamanan Informasi (SMKI) yang diterapkan sudah sesuai dengan yang diharapkan. Berdasarkan permasalahan yang ada berkaitan dengan aspek keamanan informasi (CIA) dan tujuan audit keamanan informasi, maka dilakukan audit substansi untuk menegaskan apakah hasil dari aktivitas (prosedur atau proses telah dijalankan) telah sesuai dengan yang ditargetkan atau yang diharapkan.

2. Ruang Lingkup

RRI Surabaya berkomitmen untuk menjadi instansi penyiaran publik yang dapat menyebarluaskan informasi pemerintah serta memberikan hiburan kepada masyarakat dan memberikan pendidikan.

.

SMKI RRI Surabaya diimplementasikan untuk ruang lingkup proses informasi organisasi yaitu pada bagian Pengembangan Multimedia Baru yang digunakan adalah Sistem teknologi informasi internal.

3. Penilaian Risiko

Setelah menentukan ruang lingkup proses bisnis dan TI di bagian PMB, maka auditor akan melakukan penilaian risiko agar dapat menentukan klausul yang akan digunakan untuk kegiatan audit yang akan berlangsung. Ada beberapa tahapan dalam penilaian risiko, yaitu:

1) Identifikasi Aset

Proses identifikasi aset dilakukan dengan cara membuat Tabel aset. Contoh Tabel aset dapat dilihat pada Tabel 4.2.

Tabel 4.2 Contoh Tabel Identifikasi Aset

Jenis Aset	Nama Aset
Dokumen	Informasi Penyiaran dan Hiburan
Software	Sistem Operasi (*Windows*) – (AEQ, MIKROTIK)
Hardware	Server (DATA MASTER RRI SURABAYA)
	Personal Komputer (PC) Ruang Server, Studio Siaran, Kepala Seksi, Auditor, monitoring, reporter, rec/editing

Setelah membuat Tabel identifikasi aset maka akan dilakukan proses perhitungan nilai aset untuk mengetahui nilai informasi yang dimiliki oleh organisasi. Menghitung nilai aset berdasarkan aspek Keamanan Informasi, yaitu: *confidentiality*, *integrity*, dan *availability*. Contoh Tabel penilaian aset berdasarkan kriteria keamanan informasi dapat dilihat pada Tabel 4.3, 4.4, 4.5, dan untuk lebih lengkapnya dapat dilihat pada Lampiran 3.

Tabel 4.3 Penilaian Aset Kriteria *Confidentiality*

Kriteria *Confidentiality*	Nilai *Confidentiality* (NC)
Public	0
Internal Use Only	**1**
Private	2
Confidential	3
Secret	4

(Sumber: Sarno dan Iffano, 2009)

Tabel 4.4 Penilaian Aset Kriteria *Integrity*

Kriteria *Integrity*	Nilai *Integrity* (NI)
No Impact	0
Minor Incident	**1**
General Disturbance	2
Mayor Disturbance	3
Unacceptable Damage	4

(Sumber: Sarno dan Iffano, 2009)

Tabel 4.5 Penilaian Aset Kriteria *Availability*

Kriteria *Availability*	Nilai *Availability* (NV)
Low/No Availability	0
Office Hours Availability	**1**
Strong Availability	2
High Availability	3
Very High Availability	4

(Sumber: Sarno dan Iffano, 2009)

Dari ketiga Tabel tersebut, maka akan dilakukan pemilihan nilai aset dengan penulisan huruf tebal atau *bold*. Perhitungan nilai aset menggunakan persamaan matematis dengan rumus pada (2.1):

Nilai Aset = NC + NI + NV

Jenis Aset: Perangkat Keras

Nama Aset: Server

Nilai Aset:

Confidentiality: *Internal Use Only* (NC = 1)

Integrity: *Minor Incident* (NI = 1)

Availability: *Office Hours Availability* (NV = 1)

NC + NI + NV = 1 + 1 + 1

Nilai Aset (Server) = 3

2) Identifikasi Ancaman dan Kelemahan

Proses identifikasi ancaman dan kelemahan dilakukan dengan cara membuat Tabel kemungkinan kejadian gangguan keamanan. Contoh Tabel kemungkinan gangguan keamanan dapat dilihat pada Tabel 4.6.

Tabel 4.6 Contoh Kemungkinan Gangguan Keamanan

Kejadian	Jenis	Probabilitas
Gangguan Sumber Daya	*Vulnerable*	*Low*
Gangguan Perangkat Keras	*Vulnerable*	*Medium*
Kebakaran	*Threat*	*Low*
Serangan Virus: *Trojan, Worm,* dll.	*Threat*	*High*
Penyusup atau *Hacker*	*Threat*	*Medium*
Kerusakan Data	*Vulnerable*	*Medium*
Kesalahan Pengiriman Data	*Vulnerable*	*Low*
Gangguan Petir	*Threat*	*Low*
Bencana Alam	*Threat*	*Low*
Akses Ilegal	*Threat*	*Medium*

(Sumber: Sarno dan Iffano, 2009)

Setelah melakukan identifikasi ancaman dan kelemahan, maka auditor melakukan proses penilaian terhadap ancaman aset pada PMB. Nilai probabilitas didapat dari hasil klasifikasi probabilitas. Rentang nilai probabilitas sebagai berikut:

(***Low*** **:** Nilai probabilitas 0,1 – 0,3)

(***Medium*****:** Nilai probabilitas 0,4 – 0,6)

(***High*** **:** Nilai probabilitas 0,7 – 1).

Contoh perhitungan nilai ancaman aset informasi pada bagian PMB dapat dilihat pada Tabel 4.7.

Tabel 4.7 Perhitungan Nilai Ancaman

Ancaman	**Jenis**	**Probabilitas**	**Nilai Probabilitas**
Virus: Trojan, Worm, dll.	*Threat*	*High*	0.7
Akses Ilegal	*Threat*	*High*	0.7
Kerusakan Data	*Threat*	*High*	1
Penyusup atau *Hacker*	*Threat*	*Low*	0.1
Gangguan Sumber Daya	*Vulnerable*	*Low*	0.3
Gangguan Perangkat Keras	*Vulnerable*	*Low*	0.3
Jumlah Ancaman = 6	**Jumlah Rata-Rata Probabilitas**		**3,4**

Dari hasil Tabel perhitungan nilai ancaman (NT) dapat dihitung terhadap aset server PMB dengan rumus:

NT (Server) = ∑**PO** / ∑**Ancaman**

=3,4 / 6 = 0,6

Definisi:

∑**PO:** Jumlah *Probability of Occurence*

∑**Ancaman:** Jumlah Ancaman Terhadap Informasi

3) Identifikasi Dampak (*Impact*) Kegagalan CIA

Pada langkah ini adalah mengidentifikasi dampak bisnis jika terjadi kegagalan terhadap aspek Keamanan Informasi (CIA). Contoh Tabel dampak bisnis jika terjadi kegagalan aspek Keamanan Informasi dapat dilihat pada Tabel 4.8.

Tabel 4.8 Dampak Bisnis

Kategori	Dampak		
	Low	***Medium***	***High***
Confidientiality**:** Memastikan bahwa infomasi hanya diakses oleh orang yang memiliki hak akses	Bila diakses secara ilegal dapat menyebabkan kerugian terbatas pada bagian dan pemilik informasi.	Bila diakses secara ilegal dapat menyebabkan kerugian materi, mengganggu proses siaran, dan mengurangi reputasi instansi.	Bila diakses secara ilegal dapat menyebabkan kerugian materi sangat besar, terhentinya jalanya siaran, dan konsekuensi hukum.
Integrity**:** menjaga bahwa informasi selalu utuh, akurat, dan valid.	Merubah informasi secara tidak bertanggung jawab dapat menyebabkan kerugian terbatas pada bagian dan instansi,	Merubah informasi secara tidak bertanggung jawab dapat menyebabkan kerugian materi, mengganggu kelancaran siaran, dan mengurangi reputasi instansi.	Merubah informasi secara tidak bertanggung jawab dapat menyebabkan kerugian materi sangat besar, terhentinya siaran, dan konsekuensi hukum.
Availability**:** memastikan bahwa informasi selalu tersedia jika diperlukan dan khusus diakses bagi orang yang berwenang.	Gangguan pada akses informasi dapat menyebabkan kerugian terbatas dibagian siaran dan instansi.	Gangguan pada akses informasi menyebabkan kerugian materi, mengganggu kelancaran siaran, dan mengurangi reputasi instansi.	Gangguan pada akses informasi menyebabkan kerugian materi sangat besar, terhentinya siaran, dan konsekuensi hukum.

(Sumber: Sarno dan Iffano, 2009)

4) Analisa Dampak Bisnis

Istilah BIA adalah singkatan dari analisa dampak bisnis (*Business Impact Analysis*). BIA menerangkan ketahanan proses bisnis organisasi jika informasinya terganggu. Analisa dampak bisnis dilakukan dengan cara membuat Skala Nilai BIA yang dipilih dengan huruf tebal pada tiap Tabel dan dapat dilihat pada Tabel 4.9, sedangkan contoh Tabel BIA Fasilitas Informasi yang dimiliki bagian PMB dengan mengacu pada nilai skala yang ditandai dengan huruf tebal dan dapat dilihat pada Tabel 4.10.

Tabel 4.9 Skala Nilai BIA

Batas Toleransi Gangguan	Keterangan	Nilai Skala
< dari 1 minggu	*Not Critical*	0-20
1 hari s/d 2 hari	*Minor Critical*	21-40
< dari 1 hari	*Mayor Critical*	41-60
< dari 12 jam	*High Critical*	61-80
< dari 1 jam	***Very High Critical***	**81-100**

(Sumber: Sarno dan Iffano, 2009)

Tabel 4.10 BIA Fasilitas Informasi PMB

Fasilitas Informasi	Dampak	Nilai BIA
Informasi Berita	Siaran tertunda, kepercayaan pendengar dan *stakeholder* menurun	30
Server Berita	Keterlambatan pengambilan berita siaran	55
PMB	Siaran tertunda	50
PC	Komunikasi antar bagian tertunda	22
Server	**Operasi terhenti**	**85**

5) Mengidentifikasi Level Risiko

Mengidentifikasi level risiko dapat dilakukan dengan cara membuat Tabel level risiko. Dengan Tabel level risiko kita dapat mengetahui gambaran seberapa besar risiko yang diterima organisasi jika terjadi kegagalan Keamanan Informasi. Contoh Tabel level risiko dapat dilihat pada Tabel 4.11. Didalam Tabel level risiko terdapat nilai probabilitas ancaman yang dibagi dalam 3 level penilaian, yaitu:

$0 \geq$ *Low Probability* $\leq 0{,}1$

$0{,}1 >$ *Medium Probability* $\leq 0{,}5$

$0{,}5 >$ *High Probability* $\leq 1{,}0$

Sedangkan dampak bisnis dibagi dalam 5 level penilaian, yaitu:

0 ≥ *Not Critical Impact* ≤ 20

20 > *Low Critical Impact* ≤ 40

40 > *Medium Critical Impact* ≤ 60

60 > *High Critical Impact* ≤ 80

80 > *Very High Critical Impact* ≤ 100

Tabel 4.11 Level Risiko

Probabilitas ancaman	**Dampak Bisnis (*Bussiness Impact*)**				
	***Not Critical* (20)**	***Low Critical* (40)**	***Medium Critical* (60)**	***High Critical* (80)**	***Very High Critical* (100)**
***Low* (0,1)**	*Low* 20×0,1=2	*Low* 40×0,1=4	*Low* 60×0,1=6	*Low* 80×0,1=8	*Low* 100×0,1=10
***Medium* (0,5)**	*Low* 20×0,5=10	*Medium* 40×0,5=20	*Medium* 60×0,5=30	*Medium* 80×0,5=40	*Medium* 100×0,5=50
***High* (1,0)**	*Medium* 20×1,0=20	*Medium* 40×1,0=40	*High* 60×1,0=60	*High* 80×1,0=80	*High* 100×1,0=100

(Sumber: Sarno dan Iffano, 2009)

6) Menentukan Risiko Diterima atau Perlu Pengelolaan Risiko

Pada tahapan ini akan dilakukan penilaian risiko dengan menggunakan metode matematis berdasarkan hasil pada langkah-langkah sebelumnya, yaitu:

Nilai Aset: NA

Analisa Dampak Bisnis: BIA

Nilai Ancaman: NT

Nilai Risiko dapat dihitung dengan menggunakan rumus (2.3):

***Risk Value* = NA x BIA x NT**

Nama Aset: Server

Nilai Aset (NA) = 3

Nilai BIA = 42,5

Nilai Ancaman (NT) = 0.6

Nilai Risiko = 3 x 42,5 x 0,6 = 76,5

Level Risiko Server = *High Critical*

Dari hasil tersebut, nilai risiko aset server di PMB termasuk dalam kategori *high critical* dan nilai ancaman (76,5) masuk dalam kategori *high*, maka risiko dihindari atau ditolak (*risk avoidance*) yang berarti organisasi menghindari risiko yang terjadi dengan cara menghilangkan penyebab timbulnya risiko atau organisasi menghentikan aktivitasnya jika gejala risiko muncul.

Tabel 4.12 Kriteria Penilaian Risiko

No.	Nama Aset	PA (Probabilitas Ancaman)	BP (Biaya Pemulihan)	BR (Biaya Transfer Risiko)	Nilai	Kriteria
1.	Informasi Berita	*High*	*Med*	*Med*	*Medium*	*Risk Avoidance*
2.	Server Berita	*High*	*Med*	*Med*	*Medium*	*Risk Avoidance*
3.	PMB	*Med*	*Med*	*Med*	*Medium*	*Risk Reduction*
4.	PC	*Med*	*High*	*Low*	*Low*	*Risk Transfer*
5.	Server	*High*	*Med*	*Med*	*Medium*	*Risk Avoidance*

7) Menentukan Klausul ISO 27002:2005

Setelah melakukan pemetaan risiko yang terjadi dengan kontrol keamanan ISO 27002:2005 digunakan untuk memudahkan instansi dalam memilih kontrol keamanan yang sesuai keperluan instansi dengan tiga kategori pengelompokan kontrol keamanan, yaitu: manajemen, teknikal, dan operasional. Pemetaan antara permasalahan dan klausul dapat dilihat pada Tabel 4.13 hasil rangkuman dari Tabel Kebutuhan Kontrol Keamanan dan Hubungan Klausul Kontrol Keamanan dengan aspek Keamanan Informasi (Sarno dan Iffano, 2009).

Tabel 4.13 Pemetaan Permasalahan dan Klausul

Permasalahan	Klausul Kontrol Keamanan
***Confidentiality*:** Kesalahan penyimpanan berita yang tidak sesuai dengan perencanaan. Risiko yang ditimbulkan dari sisi manajemen adalah organisasi menjadi kurang kondusif, dari sisi teknikal sarana prasarana tidak maksimal, dari sisi operasional komunikasi antar bagian terganggu.	**Manajemen:** Klausul 5 Kebijakan Keamanan.
	Manajemen: Klausul 6 Organisasi Keamanan Informasi.
	Manajemen: Klausul 7 Manajemen Aset.
	Teknikal: Klausul 8 Keamanan Sumber Daya Manusia.
	Teknikal: Klausul 9 Keamanan Fisik dan Lingkungan.
	Operasional: Klausul 10 Komunikasi dan Manajemen Operasional.
	Teknikal: Klausul 11 Kontrol Akses.
***Integrity*:** Keutuhan berita hasil liputan langsung yang diakses tidak lengkap. Risiko yang ditimbulkan adalah turunya rating siaran. Risiko yang ditimbulkan dari sisi manajemen adalah organisasi menjadi kurang kondusif, dari sisi teknikal sarana prasarana tidak maksimal, dari sisi operasional komunikasi antar bagian terganggu.	**Manajemen:** Klausul 5 Kebijakan Keamanan.
	Manajemen: Klausul 7 Manajemen Aset.
	Teknikal: Klausul 9 Keamanan Fisik dan Lingkungan.
	Operasional: Klausul 10 Komunikasi dan Manajemen Operasional.
	Operasional: Klausul 13 Manajemen Insiden Keamanan Informasi.
***Availability*:** Keterlambatan peyediaan informasi, berita, siaran langsung, hiburan, dan iklan. Risiko yang ditimbulkan dari sisi manajemen adalah organisasi menjadi kurang kondusif, dari sisi teknikal sarana prasarana tidak maksimal, dari sisi operasional komunikasi antar bagian terganggu.	**Manajemen:** Klausul 5 Kebijakan Keamanan.
	Manajemen: Klausul 7 Manajemen Aset.
	Teknikal: Klausul 9 Keamanan Fisik dan Lingkungan.
	Operasional: Klausul 10 Komunikasi dan Manajemen Operasional.
	Operasional: Klausul 13 Manajemen Insiden Keamanan Informasi.

Setelah melakukan pemetaan permasalahan dengan klausul ISO 27002:2005, selanjutnya auditor melakukan pemetaan permasalahan, proses, dan klausul yang akan digunakan untuk mengetahui kesesuaian klausul yang

digunakan untuk audit dengan kebutuhan instansi. Contoh pemetaan permasalahan dan proses dapat dilihat pada Tabel 4.14.

Tabel 4.14 Pemetaan Permasalahan dan Proses

Permasalahan	Proses	Klausul
***Confidentiality*:** Kesalahan penyimpanan berita yang tidak sesuai dengan perencanaan.	Permasalahan *confidientiality* yang ada dapat terjadi pada seksi reporter dan *rec/editing* khususnya karyawan pada saat memonitor berita atau liputan langsung. Ancaman yang memungkinkan terjadi adalah akses ilegal sesama karyawan dan kelemahan yang akan terjadi adalah kesalahan menyimpan ke *server* tex*t* karena ketidaktahuan.	5, 6, 7, 8, 9, 10, dan 11.
***Integrity*:** Keutuhan berita hasil liputan langsung yang diakses tidak lengkap.	Permasalahan *integrity* yang ada dapat terjadi pada bagian *server audio multimedia*. Berawal dari bagian *rec/editing* dan reporter saat proses menyimpan informasi ke *server text* dan berlanjut ke *server multimedia*. Ancaman yang dimungkinkan terjadi adalah akses ilegal sesama karyawan, penyusup internal (karyawan) maupun pihak ketiga, virus. Sedangkan kelemahan yang terjadi adalah kesalahan penginputan informasi, kerusakan informasi, gangguan perangkat keras, dan gangguan sumber daya.	5, 7, 9, 10, dan 13.
***Availability*:** Keterlambatan peyediaan informasi, berita, siaran langsung, hiburan, dan iklan.	Permasalahan *availability* yang ada dapat terjadi pada bagian *server audio multimedia*. Berdasarkan permasalahan yang terjadi pada proses-proses sebelumnya, pihak penyiar harus melakukan pengecekan ulang yang akhirnya menyebabkan keterlambatan penyiaran berita dan siaran langsung.	5, 7, 9, 10, dan 13.

Dari hasil pemetaan permasalahaan proses bisnis dan TI yang ada, sebagian besar memiliki dampak bisnis yang masuk dalam kategori *medium* terhadap aspek keamanan informasi (CIA):

1) *Confidentiality:* Jika informasi diakses tanpa ijin dapat menyebabkan kerugian finansial, mengganggu kelancaran siaran, mengurangi kepercayaan pendengar dan rating penyiaran.
2) *Integrity:* Merubah informasi dengan tidak bertanggung jawab dapat menyebabkan kerugian financial, mengganggu kelancaran siaran, mengurangi kepercayaan pendengar dan rating penyiaran.
3) *Availability:* Gangguan terhadap akses informasi dapat menyebabkan kerugian financial, mengganggu kelancaran siaran, mengurangi kepercayaan pendengar dan rating penyiaran.

Setelah melakukan proses pemetaan, maka hasil pemilihan klausul kontrol keamanan dengan aspek keamanan informasi dapat dilihat pada Tabel 4.15. Dari hasil pemetaan pada Tabel 4.14 ada beberapa klausul yang tidak digunakan dalam penelitian ini, yaitu: klausul 5 Kebijakan Keamanan, klausul 6 Organisasi Keamanan Informasi, klausul 7 Manajemen Aset, klausul 10 Komunikasi dan Manajemen Operasional, dan klausul 13 Manajemen Insiden Keamanan Informasi. Klausul-klausul yang tidak digunakan dalam penelitian ini dapat digunakan pada penelitian serupa berikutnya agar bagian PMB RRI Surabaya dapat mengetahui tingkat keamanan Informasi lebih detil sesuai dengan permasalahan yang terjadi.

Tabel 4.15 Hubungan Klausul dengan Aspek Keamanan Informasi

ISO 27002			Aspek Keamanan Informasi		
No.	Klausul Kontrol Keamanan	Kategori Keamanan Utama	C	I	A
8	Keamanan Sumber Daya Manusia	Aturan dan tanggung jawab keamanan	√	√	√
		Tanggung Jawab Manajemen	√		
		Pendidikan dan pelatihan keamanan informasi	√		

Tabel 4.15 (Lanjutan)

ISO 27002			Aspek Keamanan Informasi		
No.	Klausul Kontrol Keamanan	Kategori Keamanan Utama	C	I	A
		Tanggung Jawab Pemberhentian	√		
9	Fisik dan Lingkungan	Kontrol masuk fisik	√	√	√
		Keamanan kantor, ruang dan fasilitasnya	√	√	√
		Letak peralatan dan pengamanannya	√		
		Keamanan pengkabelan	√		
11	Kontrol Akses	Kebijakan kontrol akses	√		
		Manajemen password user	√		
		Tinjauan terhadap hak akses user	√		
		Penggunaan Password	√		
		Kebijakan penggunaan layanan jaringan	√		
		Sistem Manajemen Password	√		
		Pembatasan akses Informasi	√		
		Komunikasi dan terkomputerisasi yang bergerak	√		
		Teleworking	√		

(Sumber: Sarno dan Iffano, 2009)

4.1.3 Hasil pemilihan Klausul, Obyektif Kontrol dan Kontrol

Untuk melakukan audit keamanan informasi, digunakan standar ISO 27002:2005 dan beberapa klausul sebagai acuan dalam pelaksanaan audit terdapat pada Tabel 4.16. Adapun dalam menetapkan klausul, obyektif kontrol dan kontrol yang disesuaikan berdasarkan 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, wawancara dan review pada PMB.

Tabel 4.16 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	a. 8.1.1 Aturan dan tanggung jawab keamanan

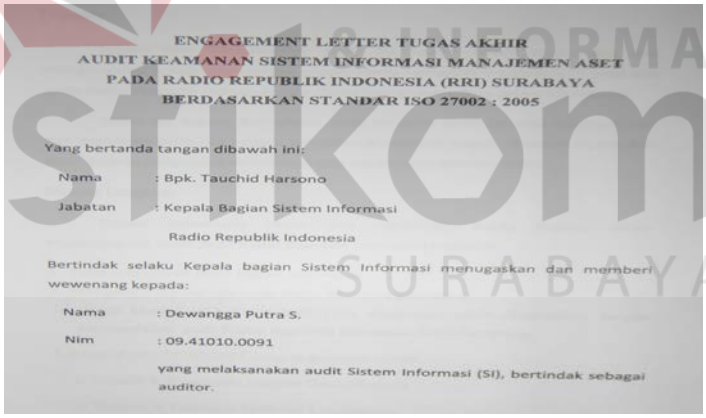
Tabel 4.16 (Lanjutan)

No.	Klausul	Objektif Kontrol	Kontrol
		Pegawai c. 8.3 Pemberhentian atau pemindahan pegawai	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 pengamanannya 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 Pengguna 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 pengguna 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

4.1.4 *Engagement Letter*

Engagement Letter merupakan surat perjanjian kedua belah pihak antara auditor dengan client sebagai bentuk kesepakatan. Pada Gambar 4.3 merupakan hasil potongan *Engagement Letter*. Adapun surat perjanjian atau *Engagement Letter* ada pada lampiran 1 dan berisi poin sebagai berikut.

a. Peran auditor
b. Tujuan auditor
c. Tugas & tanggung jawab auditor
d. Kewenangan auditor
e. Kode etik auditor
f. Ruang lingkup auditor
g. Waktu pelaksanaan



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

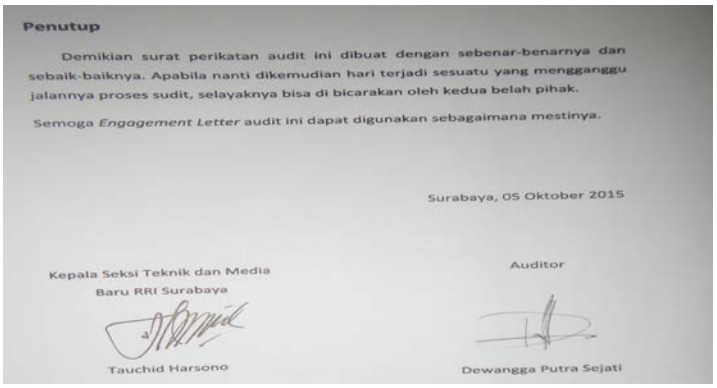
Yang bertanda tangan dibawah ini:

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.



Penutup

Demikian surat perikatan audit ini dibuat dengan sebenar-benarnya dan sebaik-baiknya. Apabila nanti dikemudian hari terjadi sesuatu yang mengganggu jalannya proses sudit, selayaknya bisa di bicarakan oleh kedua belah pihak.

Semoga *Engagement Letter* audit ini dapat digunakan sebagaimana mestinya.

Surabaya, 05 Oktober 2015

Kepala Seksi Teknik dan Media Baru RRI Surabaya

Tauchid Harsono

Auditor

Dewangga Putra Sejati

Gambar 4.3 Hasil potongan *Engagement Letter*

4.2 Hasil Persiapan Audit

Tahap hasil persiapan Audit Keamanan Informasi dilakukan dengan cara menyusun *Audit Working Plan* (AWP), penyampaian kebutuhan data audit, membuat pernyataan, melakukan pembobotan, membuat pertanyaan. Pernyataan yang telah dibuat berdasarkan standar ISO 27002:2005 dan pertanyaan yang telah dibuat berdasarkan pernyataan.

4.2.1 Hasil Penyusunan *Audit Working Plan*

Ouput dari penyusunan *Audit Working Plan* (AWP) berupa jadwal kerja. Jadwal kerja dimulai dari awal kegaitan sampai akhir kegiatan dimana dapat dilihat pada Tabel 4.17.

Tabel 4.17 *Audit Working Plan* Secara Keseluruhan

No.	Nama Pekerjaan	Durasi	Mulai (MM/DD/YY)	Selesai (MM/DD/YY)
1.	Total Hari Audit	317 hari	Kamis, 10/01/15	Jumat, 09/23/16
2.	Perencanaan Audit	152 hari	Kamis, 10/01/15	Senin, 03/14/16
3.	Persiapan Audit	17 hari	Selasa, 03/15/16	Kamis, 03/31/16
4.	Pelaksanaan Audit	21 hari	Jumat, 04/01/16	Kamis, 04/21/16
5.	Pelaporan Audit	106 hari	Jumat, 04/22/16	Jumat, 09/23/16

4.2.2 Hasil Penyampaian Kebutuhan Data

Pada tahap persiapan audit, setelah membuat AWP maka proses selanjutnya adalah menyampaikan kebutuhan data yang diperlukan kepada *auditee* untuk penunjang pemeriksaan auditor. Fungsinya dalam menyampaikan kebutuhan data sebelumnya agar auditor lebih mudah dan lebih cepat dalam memeriksa pada tahap pelaksanaannya sehingga penyampaian kebutuhan data bisa dipersiapkan sebelumnya. Adapun penyampaian kebutuhan data dapat dilihat pada Tabel 4.18 dan lebih detailnya berada pada Lampiran 3

Tabel 4.18 Lampiran Kebutuhan Data Audit Secara Umum

Lampiran Permintaan Kebutuhan Data/Dokumen						
No.	Data yang diperlukan	Ketersediaan Data		Keterangan	Tanda Tangan	
		Ada	Tidak ada		Auditee	Auditor
1	Profil perusahaan	√		Ada berdasarkan wawancara dengan pegawai RRI Sby		
2	Struktur organisasi RRI Sby	√		Ada datanya terletak Di gambar stuktur organisasi		
3	*Job description* pegawai di RRI Sby	√		Ada tertuang di TUPOKSI RRI Sby		
4	Alur proses bisnis insatansi	√		Ada tertuang pada lampiran STUDIO INTEGRASI		
5	Dokumen kebijakan keamanan sistem informasi		√			

4.2.3 Hasil Pernyataan

Pada Proses selanjutnya pada tahapan persiapan audit dilakukan dengan membuat pernyataan berdasarkan kontrol keamanan yang terdapat pada setiap klausul yang telah ditetapkan berdasarkan standar ISO 27002. Pada setiap kontrol keamanan dapat ditentukan pernyataan yang mendiskripsikan implementasi dan pemeliharaan kontrol keamanan tersebut. Contoh pernyataan pada klausul 8 (delapan) Keamanan Sumber Daya Manusia dengan obyek kontrol 8.1.1 aturan dan tanggung jawab keamanan (*Rules and Responsibilities*) dapat dilihat pada Tabel 4.19, dan selengkapnya dapat dilihat pada Lampiran 4 Pernyataan Klausul 8,9,11.

Tabel 4.19 Pernyataan Klausul 8.1.1 Aturan dan Tanggung jawab Keamanan (*Roles and Responsibilities*)

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

Pernyataan berdasarkan standar ISO 27002:2005 digunakan untuk memudahkan auditor sebagai acuan membuat pertanyaan untuk wawancara audit keamanan sistem informasi dari beberapa contoh klausul yaitu klausul 8 (Delapan) Keamanan Sumber Daya Manusia dengan obyek kontrol 8.1.1 (Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*)) membahas tentang aturan dan tanggung jawab keamanan sehingga bila semua aspek aturan dan tanggung jawab keamanan terdapat pada bagian PMB maka dapat menjadi standar keamanan sumber daya manusia pada bagian tersebut, klausul 9 (Sembilan) Keamanan Fisik dan Lingkungan dengan obyek kontrol 9.1.2 kontrol masuk fisik (*Physical entry controls*) membahas tentang kontrol masuk fisik sehingga bila semua aspek kontrol masuk fisik terdapat pada bagian PMB maka dapat menjadi standar keamanan fisik dan lingkungan pada bagian tersebut, klausul 11 (Sebelas) Kontrol Akses dengan obyek kontrol 11.3.1 Penggunaan kata sandi (*Password Use*) membahas tentang penggunaan password sehingga bila semua aspek

penggunaan password terdapat pada bagian PMB maka dapat menjadi standar kontrol akses dibagian tersebut.

4.2.4 Hasil Pembobotan Pernyataan

Setelah membuat pernyataan, maka langkah selanjutnya adalah melakukan pengukuran pembobotan pada setiap pernyataan. Pembobotan dilakukan berdasarkan perhitungan, dengan membagi tingkat pembobotan dalam manajemen menjadi 3 (tiga), yaitu: rendah, cukup dan tinggi yang telah disesuaikan dengan kondisi bagian PMB dan kesepakatan dengan pihak Kepala Seksi PMB dengan kriteria pada Tabel 4.20, sebagai berikut:

Tabel 4.20 Tingkat Kepentingan dalam Pembobotan Pernyataan

Risiko	Bobot
Rendah	0,1 - 0,3
Sedang	0,4 - 0,6
Tinggi	0,7 - 1,0

(Sumber: Sarno, 2009)

Pembobotan ditentukan dari panduan implementasi dan tingkat kepentingannya bagi organisasi. Pernyataan yang mendapatkan pembobotan dengan resiko *high* berarti pernyataan tersebut sangat penting untuk diterapkan pada perusahaan. Untuk pernyataan dengan bobot resiko *medium* berarti pernyataan tersebut tetap diterapkan meskipun resiko yang akan terjadi apabila ada ancaman keamanan tidak sebesar dengan bobot resiko *high*. Pernyataan dengan resiko *low* berarti pernyataan tersebut tidak terlalu wajib untuk diterapkan namun apabila diterapkan akan menambah keamanan pada sistem.

Beberapa contoh pembobotan yang ada dalam klausul 8 (delapan) Keamanan Sumber Daya Manusia dengan obyek kontrol 8.1.1 aturan dan

tanggung jawab keamanan (*Roles and Responsibilities*) dapat dilihat pada Tabel 4.21, dan untuk selengkapnya dapat dilihat pada Lampiran 4 Pernyataan dan Pembobotan Klausul 8,9, dan 11.

Tabel 4.21 Pembobotan Klausul 8.1.1 Aturan dan Tanggung Jawab Keamanan (*Roles and Responsibilities*)

PEMBOBOTAN PERNYATAAN AUDIT KEAMANAN INFORMASI KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)	**Auditor: Dewangga Putra Sejati** **Auditee: Tauchid Harsono** **NIP. 19651018 198503 1 003** **Tanggal : 15 Maret 2016** **Tanda tangan:**		
PEMBOBOTAN 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	Bobot		
		Rendah (0,1-0,3)	Sedang (0,4-0,6)	Tinggi (0,7-1,0)
1.	Terdapat peraturan pada proses penerimaan pegawai pada RRI Sby	0,3		
2.	Terdapat prosedur kebijakan tanggung jawab pegawai terhadap perlindungan aset	0,3		
3.	Terdapat peran dan tanggung jawab dalam melaksanakan dan bertindak sesuai dengan kebijakan keamanan informasi organisasi yang ada		0,6	
4.	Terdapat kepastian bahwa tanggung jawab pegawai benar benar sudah diberikan demi melindungi keamanan informasi		0,5	

Dari hasil pembobotan untuk klausul 8 (Delapan) Keamanan Sumber Daya Manusia dengan obyek kontrol 8.1.1 aturan dan tanggung jawab keamanan (*Roles and Responsibilities*) didapatkan pentingnya tanggung jawab pegawai untuk PMB, sehingga pihak PMB harus lebih memperhatikan aturan dan

tanggung jawab pada bagian tersebut. Untuk klausul 9 (Sembilan) Keamanan Fisik dan Lingkungan dengan obyek kontrol 9.1.2 kontrol masuk fisik (*Physical entry controls*) didapatkan pentingnya kontrol masuk fisik untuk ruang PMB, karena tidak semua orang bisa memasuki wilayah aman terutama wilayah pemrosesan informasi, dan pada ruangan pemrosesan informasi tersebut rawan sekali apabila tidak benar-benar dijaga secara khusus sehingga pihak PMB harus lebih memperhatikan kontrol masuk fisik untuk keamanan fisik dan lingkungan. Untuk klausul 11 (Sebelas) Kontrol Akses dengan obyek kontrol 11.3.1 penggunaan kata sandi (*Password Use*) didapatkan pentingnya penggunaan kata sandi untuk bagian PMB, sehingga karyawan harus lebih memperhatikan penggunaan kata sandi pada bagian PMB.

4.2.5 Hasil Pertanyaan

Setelah melakukan pembobotan pernyataan langkah selanjutnya adalah membuat pertanyaan. Pertanyaan yang dibuat mengacu pada pernyataan yang ada dimana satu pernyataan bisa memiliki lebih dari satu pertanyaan, hal tersebut dikarenakan setiap pertanyaan harus mewakili pernyataan pada saat dilakukan wawancara. Pertanyaan pada Tabel didasarkan pada pernyataan yang telah disesuaikan dengan standar ISO 27002. Contoh pertanyaan pada klausul 8 (Delapan) Keamanan Sumber Daya Manusia dengan obyek kontrol 8.1.1 aturan dan tanggung jawab keamanan (*Roles and Responsibilities*), dapat dilihat pada Tabel 4.22, dan untuk selengkapnya dapat dilihat pada Lampiran 6 Pertanyaan Klausul 8, 9, dan 11.

Tabel 4.22 Hasil Pertanyaan Klausul 8.1.1 Aturan dan Tanggung Jawab Keamanan (*Roles and Responsibilities*)

AUDIT KEAMANAN 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*)	
1	Terdapat peraturan pada proses penerimaan pegawai di RRI Sby
	P: Adakah peraturan khusus pada proses penerimaan pegawai di RRI Sby? J: Ada, dengan test wawancara dari pihak terkait (SMA, SMK, dan Perguruan tinggi) P: Bagaimana peraturan pada proses penerimaan pegawai di RRI Sby ? J: Pelamar membawa lamaran kerja lalu menunggu panggilan dari RRI Sby dan selanjutnya wawancara P: Adakah dokumentasi peraturan pada proses penerimaan pegawai di RRI Sby? J: Ada, di bagian SDM. Lampiran: foto penerimaan pegawai
2	Terdapat prosedur kebijakan tanggung jawab pegawai terhadap perlindungan aset
	P: Apakah organisasi telah melakukan perlindungan terhadap aset pada peran dan tanggung jawab pegawai di RRI Sby? J: Ya, dengan menjalankan tugas sesuai tugas pokok siaran (TUPOKSI) P: Siapakah yang membuat perlindungan aset yang sesuai dengan peran dan tanggung jawab pegawai tersebut? J: seluruh pegawai RRI SBY P: Apakah ada dokumentasinya dari perlindungan aset tersebut ? J: Hasil laporan tiap bulan.

4.3 Hasil Pelaksanaan Audit

Pada tahap ini langkah-langkah yang dilakukan yaitu: 1. Dokumen hasil wawancara, 2. Dokumen hasil pemeriksaan data, 3. Hasil uji kematangan, dan 4. Daftar temuan dan rekomendasi. Keluaran hasil pada tahapan ini adalah pertanyaan dan jawaban dari *auditee*, hasil pemeriksaan auditor, hasil uji

kematangan, temuan dan rekomendasi, bukti foto audit yang dapat dilihat pada Lampiran 8 Dokumen hasil pemeriksaan.

4.3.1 Dokumen Hasil Wawancara

Pada proses wawancara, auditor melakukan wawancara berdasarkan pertanyaan yang telah dibuat. Wawancara dilakukan berdasarkan pertanyaan yang telah dibuat oleh auditor. Wawancara ditujukan kepada pihak yang terlibat didalamnya yaitu *auditee.* Beberapa contoh hasil wawancara terdapat pada klausul 8 (Delapan) Keamanan Sumber Daya Manusia dengan obyek kontrol 8.1.1 aturan dan tanggung jawab keamanan (*Roles and Responsibilities*), dapat dilihat pada Tabel 4.22, dan selengkapnya pada Lampiran 7 Dokumen wawancara pemeriksaan data.

Tabel 4.22 Wawancara Klausul8.1.1 Aturan dan Tanggung Jawab Keamanan (*Roles and Responsibilities*)

KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)	Auditor: Dewangga Putra Sejati Auditee: GILANG SETIO NUGROHO NIP. 19890522 201301 NO1 Tanggal : 22 Maret 2016 Tanda tangan:
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*)	
1	Terdapat peraturan pada proses penerimaan pegawai di RRI Sby
	P: Adakah peraturan khusus pada proses penerimaan pegawai di RRI Sby? J: Ada, dengan test wawancara dari pihak terkait (SMA, SMK, dan Perguruan tinggi) P: Bagaimana peraturan pada proses penerimaan pegawai di RRI Sby ? J: Pelamar membawa lamaran kerja lalu menunggu panggilan dari RRI Sby dan selanjutnya wawancara P: Adakah dokumentasi peraturan pada proses penerimaan pegawai di RRI Sby J: Tidak ada.

Tabel 4.22 (Lanjutan)

KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)	Auditor: Dewangga Putra Sejati Auditee: GILANG SETIO NUGROHO NIP. 19890522 201301 NO1 Tanggal : 22 Maret 2016 Tanda tangan:
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*)	
2	Terdapat prosedur kebijakan tanggung jawab pegawai terhadap perlindungan aset
	P: Apakah organisasi telah melakukan perlindungan terhadap aset pada peran dan tanggung jawab pegawai di RRI SBY? J: Ya, dengan menjalankan tugas sesuai tugas pokok siaran (TUPOKSI) P: Siapakah yang membuat perlindungan aset yang sesuai dengan peran dan tanggung jawab pegawai tersebut? J: seluruh pegawai RRI SBY P: Apakah ada dokumentasinya dari perlindungan aset tersebut ? J: Hasil laporan tiap bulan.
3	Terdapat peran dan tanggung jawab dalam melaksanakan dan bertindak sesuai dengan kebijakan keamanan informasi organisasi yang ada
	P: Apakah peran dan tanggung jawab pegawai sudah sesuai dengan kebijakan keamanan informasi yang diterapkan instansi? J: Sudah, dengan berjalanya siaran sesuai TUPOKSI P: Siapa yang membuat kebijakan keamanan informasi yang mengatur peran dan tanggung jawab pegawai tersebut? J: dibagian PMB adalah Pak Tauchid Harsono yang nantinya dilaksankan pelaksana P: Apakah terdapat dokumentasi kebijakan keamanan informasi insatansi yang khusus mengatur peran dan tanggung jawab pegawai? J: Iya ada sudah tertulis, di TUPOKSI

Tabel 4.22 (Lanjutan)

KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)	Auditor: Dewangga Putra Sejati Auditee: GILANG SETIO NUGROHO NIP. 19890522 201301 NO1 Tanggal : 22 Maret 2016 Tanda tangan:
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*)	
4	Terdapat kepastian bahwa tanggung jawab pegawai benar benar sudah diberikan demi melindungi keamanan informasi
	P: Apakah telah dilakukan pelaporan apabila ada suatu ancaman yang beresiko bagi keamanan organisasi instansi? J: Sudah dilaporkan. P: Siapa yang bertanggung jawab atas laporan peristiwa yang memiliki potensi resiko pada keamanan informasi yang ada? J: Masing-masing pegawai yang bertugas P: Apakah terdapat dokumentasi atas laporan peristiwa yang berpotensi beresiko pada keamanan informasi yang ada? J: ada, buku laporan catatan kerja

4.3.2 Dokumen Hasil Pemeriksaan Data

Setiap langkah pemeriksaan yang ada dalam program audit dilaksanakan oleh auditor dengan menggunakan satu atau lebih teknik audit yang sesuai dan disertai data bukti pendukung yang memadai. Wawancara dan observasi dilakukan untuk mendapatkan bukti atau temuan mengenai fakta terkait dengan masalah yang ada. Bukti-bukti tersebut berupa foto, dokumen, dan data di RRI Surabaya. Beberapa contoh dokumen pemeriksaan pada klausul 8 (Delapan) Keamanan Sumber Daya Manusia dengan obyek kontrol 8.1.1 aturan dan tanggung jawab keamanan, dokumen pemeriksaan data audit dapat dilihat pada

Tabel 4.23 dan selengkapnya dapat dilihat di Lampiran 8 Dokumen hasil pemeriksaan data.

Tabel 4.23 Dokumen Hasil Pemeriksaan Data Pada Klausul 8.1.1 Aturan dan Tanggung Jawab

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 Dengan cara: 1. Wawancara. mengenai tanggung jawab pegawai terhadap perlindungan aset 2. Didapatkan keterangan mengenai perlindungan aset	Telah diperiksa bahwa dilakukan perlindungan aset oleh bagian PMB. Dan dokumentasinya juga berada di bagian tersebut.	Terdapat dokumen tanggung jawab pegawai dalam melindungi aset oleh bagian PMB. Lampiran: SKP Basuki.

Tabel 4.23 (Lanjutan)

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
3.	Identifikasi peran dan tanggung jawab dalam bertindak sesuai dengan kebijakan keamanan informasi organisasi yang ada Dengan cara: 1. Wawancara mengenai peran dan tanggung jawab sesuai kebijakan yang berlaku 2. Didapatkan dokumentasi mengenai kebijakan keamanan informasi perusahaan yang khusus mengatur peran dan tanggung jawab pegawai	Telah dilakukan pemeriksaan bahwa peran dan tanggung jawab pegawai telah tertuang pada tupoksi pegawai di dalam dokumen peraturan tentang tanggung jawab yang dimiliki masing masing pihak seperti pegawai, pegawai non PNS.	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: TUPOKSI PNS, TUPOKSI non PNS

Tabel 4.23 (Lanjutan)

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
4.	Identifikasi tentang kepastian mengenai tanggung jawab pegawai sudah diberikan demi melindungi keamanan informasi Dengan cara: 1. Wawancara mengenai tanggung jawab pegawai demi perlindungan keamanan informasi 2. Didapatkan dokumentasi atau laporan mengenai peristiwa yang berpotensi beresiko pada keamanan informasi	Telah dilakukan pemeriksaan pada pelaporan jika terjadi suatu peristiwa yang memiliki resiko pada keamanan informasi yang ada oleh pihak yang terkait, dan dokumentasinya tertuang dalam log harian.	Dokumentasi tentang kepastian tanggung jawab pegawai dalam melindungi keamanan informasi tertuang dalam LCK pegawai masing-masing. Lampiran: dokumen SKP

4.3.3 Hasil Uji Kematangan

Berdasarkan analisa dari wawancara dengan *auditee*, pemeriksaan, dan pengumpulan bukti, maka diperoleh hasil uji kepatutan dari tingkat kematangan untuk masing-masing kontrol dapat dilihat pada tabel 4.24 dan tingkat kematangan tersebut diperoleh dari masing-masing analisa dapat dilihat pada kerangka kerja perhitungan tingkat kepatutan pada lampiran 10. Kesimpulan hasil tingkat kematangan audit keamanan informasi adalah sebagai berikut:

Tabel 4.24 Tingkat Kematangan 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)

a. Hasil tingkat kepatutan Klausul 8 Keamanan Sumber Daya Manusia

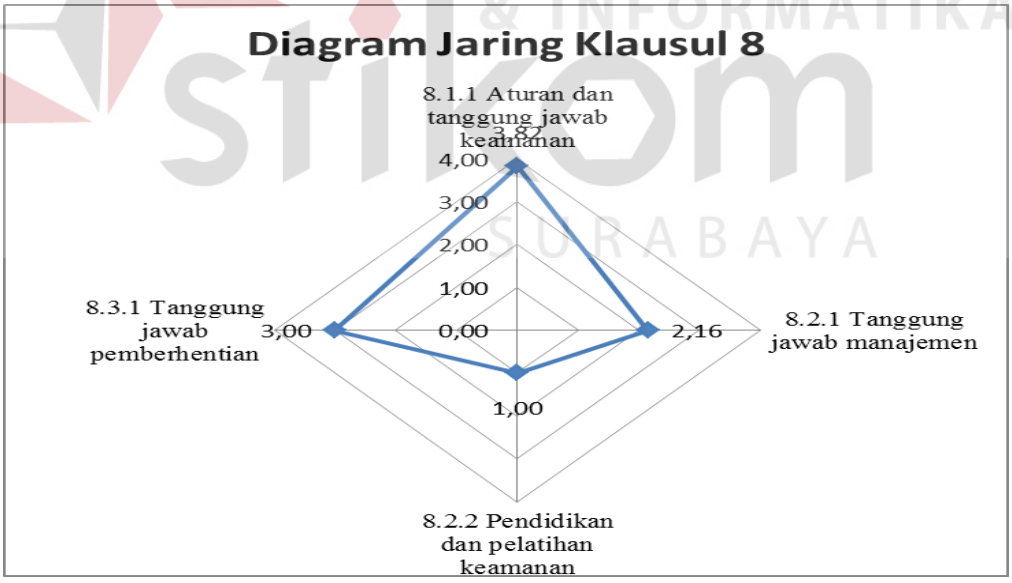
Hasil dari proses perhitungan tingkat kepatutan pada klausul 8 keamanan sumber daya manusia adalah 2,80 yaitu *managed.* Hasil tersebut menunjukkan bahwa proses keamanan sumber daya manusia yang ada masih dalam pengembangan dan dokumentasi masih sedikit. Hal ini dapat dilihat dengan adanya beberapa prosedur yang belum terdokumentasi dan kontrol yang masih belum dipertegas misalnya mematuhi prosedur keamanan informasi, belum adanya pelatihan kesadaran keamanan informasi, tidak adanya dokumen yang mengatur mengenai kesadaran akan keamanan informasi. Hasil perhitungan tersebut dapat dilihat pada Tabel 4.25. hasil perhitungan tingkat kepatutan pada klausul 8 keamanan sumber daya manusia dapat dipresentasikan dalam bentuk diagram jaring dan dapat dilihat pada Gambar 4.4.

Tabel 4.25 Hasil tingkat kepatutan Klausul 8 Keamanan Sumber Daya Manusia

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

Tabel 4.25 (Lanjutan)

Klausul	Obyektif Kontrol	Kontrol keamanan	Tingkat Kemampuan	Rata-rata obyektif kontrol
8 Keamanan sumber daya manusia	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 4.4 Representasi Nilai *Maturity Level* Klausul 8 Keamanan Sumber Daya Manusia

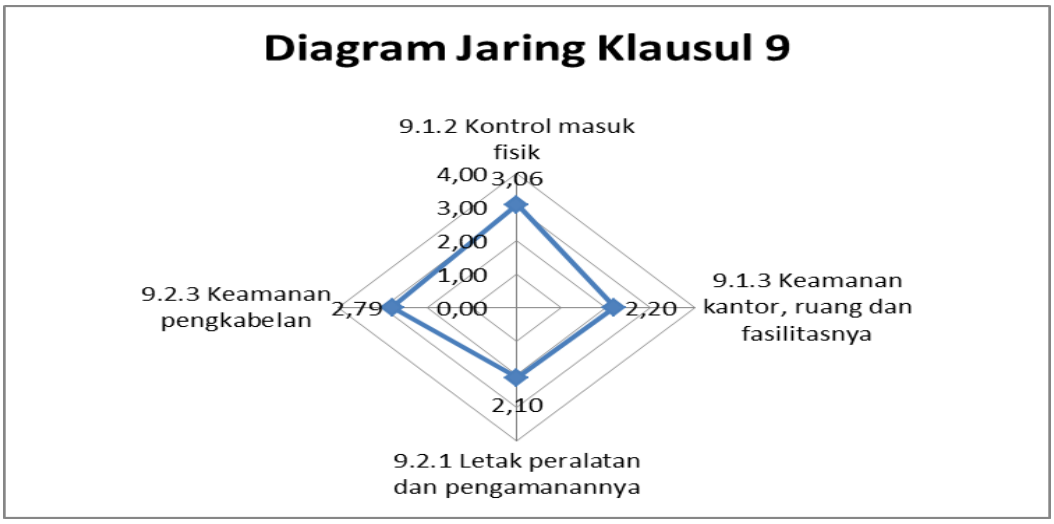
b. Hasil *Maturity Level* Klausul 9 Wilayah Aman

Hasil dari proses perhitungan *Maturity Level* pada klausul 9 wilayah aman adalah 2,54 yaitu *managed*. Hasil tersebut menunjukkan bahwa proses

keamanan wilayah yang ada masih dalam pengembangan dan memiliki dokumentasi yang terbatas. Hal tersebut dapat dilihat dengan adanya beberapa prosedur yang belum terdokumentasi dan masih adanya kontrol yang belum dilakukan misalnya pemasangan kabel yang belum rapi, CCTV yang masih belum sempurna, tidak adanya penjaga di ruang PMB saat ditinggalkan, belum adanya *intruder detection* yang memadai, dan lain-lain. Hasil perhitungan tersebut dapat dilihat pada Tabel 4.25 dan hasil perhitungan *maturity level* pada klausul 9 wilayah aman dapat direpresentasikan dalam bentuk diagram jaring yang dapat dilihat pada Gambar 4.5.

Tabel 4.26 Hasil *Maturity Level* Klausul 9 Wilayah Aman

Klausul	Obyektif Kontrol	Kontrol keamanan	Tingkat Kemampuan	Rata-rata obyektif kontrol
9 Keamanan fisik dan lingkungan	9.1 Wilayah Aman	9.1.2 Kontrol masuk fisik	3,06	2,63
		9.1.3 Keamanan kantor, ruang dan fasilitasnya	2,20	
	9.2 Keamanan Peralatan	9.2.1 Letak peralatan dan pengamanannya	2,10	2,45
		9.2.3 Keamanan pengkabelan	2,79	
Maturity Level Klausul 9				2,54



Gambar 4.5 Representasi Nilai *Maturity Level* Klausul 9 Wilayah Aman

c. Hasil *Maturity Level* Klausul 11 Kontrol Akses

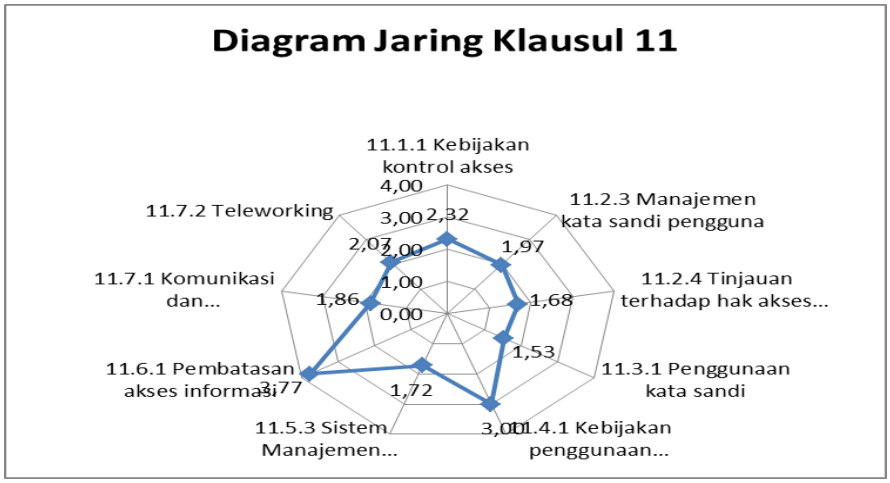
Hasil dari proses perhitungan *maturity level* pada klausul 11 kontrol akses adalah 2,21 yaitu *managed*. Hasil tersebut menunjukan bahwa kontrol akses masih dalam pengembangan dan memiliki dokumentasi yang terbatas. Hal tersebut dapat dilihat dari adanya beberapa prosedur yang belum terdokumentasi dan adanya persyaratan yang belum dilakukan misalnya penyampaian informasi secara lisan, tidak adanya dokumen yang mengatur tentang persyaratan keamanan informasi, tidak adanya kata sandi sementara, tidak terdapat verifikasi identitas untuk pemberian kata sandi baru, peninjauan hak akses pengguna terkesan pasif karena menunggu komplain, kata sandi lama masih digunakan karena masih belum ada penyimpangan, dan lain-lain. Hasil perhitungan tersebut dapat dilihat pada Tabel 4.27 dan hasil perhitungan *maturity level* pada klausul 11 kontrol akses dapat direpresentasikan dalam bentuk diagram jaring yang dapat dilihat pada Gambar 4.6.

Tabel 4.27 Hasil *Maturity level* Klausul 11 Kontrol Akses

Klausul	Obyektif Kontrol	Kontrol keamanan	Tingkat Kemampuan	Rata-rata obyektif kontrol
11 Kontrol akses	11.1 Persyaratan Bisnis Untuk Akses Kontrol	11.1.1 Kebijakan kontrol akses	2,32	2,32
	11.2 Manajemen Akses User	11.2.3 Manajemen kata sandi pengguna	1,97	1,83
		11.2.4 Tinjauan terhadap hak akses pengguna	1,68	
	11.3 Tanggung Jawab Pengguna	11.3.1 Penggunaan kata sandi	1,53	1,53
	11.4 Kontrol Akses Jaringan	11.4.1 Kebijakan penggunaan layanan jaringan	3	3,00
	11.5 Kontrol Akses Sistem Operasi	11.5.3 Sistem Manajemen Password	1,72	1,72

Tabel 4.27 Hasil *Maturity level* Klausul 11 Kontrol Akses (Lanjutan)

Klausul	Obyektif Kontrol	Kontrol keamanan	Tingkat Kemampuan	Rata-rata obyektif kontrol
	11.6 Kontrol Akses Informasi dan Aplikasi	11.6.1 Pembatasan akses informasi	3,77	3,77
	11.7 Komputasi Bergerak dan Bekerja Dari Lain Tempat	11.7.1 Komunikasi dan terkomputerisasi yang bergerak	1,86	1,97
		11.7.2 Teleworking	2,07	
***Maturuty Level* Klausul 11**				**2,30**



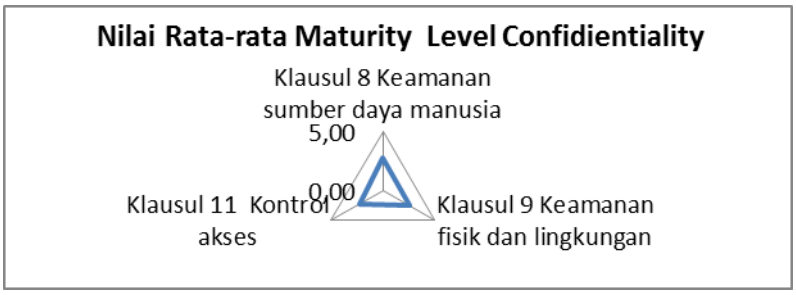
Gambar 4.6 Representasi Nilai *Maturity Level* Klausul 11 Kontrol Akses

d. Hasil *Maturity Level Confidientiality*

Pada proses perhitungan seluruh klausul didapatkan nilai tingkat kematangan 2,55 yaitu *managed*. Hal ini menunjukkan bahwa proses keamanan informasi di RRI Surabaya masih dalam pengembangan dalam mengelola suatu proses informasi. Hasil perhitungan tersebut dapat dilihat dalam Tabel 4.28 dan hasil representasi dari semua klausul dapat dilihat pada Gambar 4.7

Tabel 4.28 Hasil Rata-rata *Maturity Level Confidientiality*

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



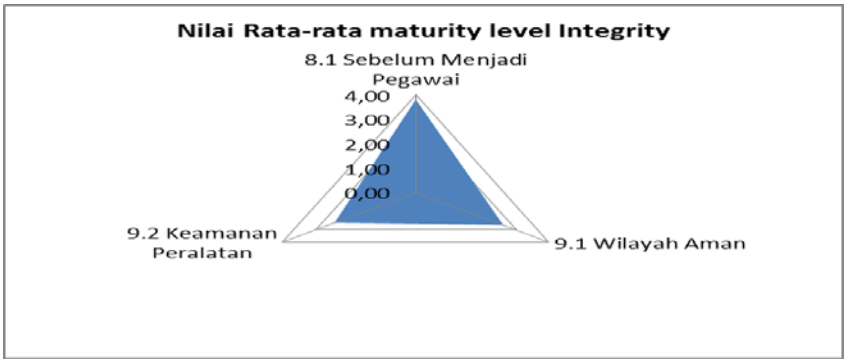
Gambar 4.7 Representasi Rata-Rata *Maturity Level Confidientiality*

e. Hasil *Maturity Level Integrity*

Hasil dari proses perhitungan tingkat kematangan aspek keamanan *Integrity* adalah 2.97 *managed*. Hasil tersebut menunjukkan bahwa sebagian besar proses keamanan informasi pada bagian PMB RRI Surabaya sudah direncanakan dan dilaksanakan dengan dokumentasi yang terbatas. Hasil perhitungan tersebut dapat dilihat dalam Tabel 4.29 dan hasil representasi dari semua klausul dapat dilihat pada Gambar 4.8

Tabel 4.29 Hasil Rata-Rata *Maturity Llevel Integrity*

Klausul	Deskripsi	Tingkat Kematangan
(Klausul 8)	8.1 Sebelum Menjadi Pegawai	3,82
(Klausul 9)	9.1 Wilayah Aman	2,63
(Klausul 9)	9.2 Keamanan Peralatan	2,45
Nilai Rata-Rata Tingkat Kematangan (*Integrity*)		2,97



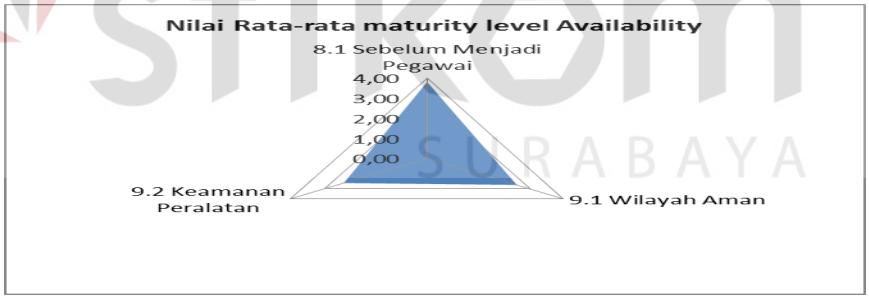
Gambar 4.8 Representasi rata-rata *maturity level integrity*

f. Hasil *Maturity Level Availability*

Hasil dari proses perhitungan tingkat kematangan aspek keamanan *availability* adalah 2,97 *managed*. Hasil tersebut menunjukkan bahwa sebagian besar proses keamanan informasi pada bagian PMB RRI Surabaya sudah direncanakan dan dilaksanakan dengan dokumentasi yang terbatas. Hasil perhitungan tersebut dapat dilihat dalam Tabel 4.30 dan hasil representasi dari semua klausul dapat dilihat pada Gambar 4.9

Tabel 4.30 Hasil Rata-Rata *Maturity Level Availability*

Klausul	Deskripsi	Tingkat Kematangan
(Klausul 8)	8.1 Sebelum Menjadi Pegawai	3,82
(Klausul 9)	9.1 Wilayah Aman	2,63
(Klausul 9)	9.2 Keamanan Peralatan	2,45
Nilai Rata-Rata Tingkat Kematangan (*Availability*)		2,97



Gambar 4.9 Representasi Rata-Rata *Maturity Level Availability*

4.3.4 Daftar Temuan dan Rekomendasi

Penyusunan temuan dan rekomendasi sebagai hasil evaluasi dari pelaksanaan audit keamanan informasi ini muncul setelah dilakukan pembandingan antara apa yang seharusnya dilakukan dengan proses yang sedang berlangsung pada instansi penyiaran. Dari hasil temuan tersebut kemudian

dilaksanakan rekomendasi yang merupakan rincian temuan serta rekomendasi yang diberikan untuk perbaikan proses keamanan sistem informasi ke depannya. Contoh temuan dan rekomendasi pada klausul 8 (Delapan) Keamanan Sumber Daya Manusia. Keterangan hasil temuan dan rekomendasi dapat dilihat pada Tabel 4.31, dan untuk selengkapnya dapat dilihat pada Lampiran 9 temuan dan rekomendasi audit.

Tabel 4.31 Daftar Temuan dan Rekomendasi Pada Klausul 8 Keamanan Sumber Daya Manusia

TEMUAN AUDIT KEAMANAN INFORMASI				Auditor : Dewangga Putra S. Auditee : GILANG SETIO NUGROHO NIP : 19890522 201301 NO1
ASPEK : KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)				Tanggal : 22 Mar-09 Apr 2016 Tanda Tangan :
No	Pernyataan	Temuan	Referensi, Penyebab, Risiko dan Rekomendasi	Tanggapan dan Komitmen Penyelesaian
1.	Terdapat pemberitahuan dari pihak manajemen kepada pegawai mengenai peran dan tanggung jawab keamanan informasi sebelum akses ke informasi yang sensitif.	Instansi hanya terdapat pemberitahuan secara lisan kepada bagian yang berhak mengakses informasi mengenai pentingnya prosedur keamanan informasi sebelum mengakses data dari ruang penyimpanan informasi. Dalam tidak terdapat dokumen yang mengatur mengenai	Referensi: ISO 27002 8.2.1 Tanggung jawab manajemen. Pernyataan 8.2.1 no.2 Penyebab: Bagian PMB RRI Sby belum menyadari pentingnya keamanan informasi untuk instansi. Risiko: Kebocoran informasi, penyalahgunaan informasi, pelanggaran hak akses yang mengancam kinerja pegawai lain.	Tanggapan : Tidak adanya prosedur atau dokumen khusus untuk mengatur tentang akses informasi yang sensitif ke server namun ada teguran dari kepala seksi masing-masing bagian apabila bertindak melampaui batas. Komitmen: Pihak RRI Sby khususnya kepala seksi bagian PMB akan membuat catatan untuk pembuatan prosedur atau dokumen peraturan khusus

Tabel 4.31 (Lanjutan)

TEMUAN AUDIT KEAMANAN INFORMASI				Auditor : Dewangga Putra S. Auditee : GILANG SETIO NUGROHO NIP : 19890522 201301 NO1
ASPEK : KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)				Tanggal : 22 Mar-09 Apr 2016 Tanda Tangan :
No	Pernyataan	Temuan	Referensi, Penyebab, Risiko dan Rekomendasi	Tanggapan dan Komitmen Penyelesaian
		prosedur keamanan informasi.	Rekomendasi: a. Pihak manajemen seharusnya dapat mengetahui peran dan tanggung jawab keamanan informasi b. Pihak kepala seksi seharusnya menetapkan prosedur keamanan informasi c. Implementasi prosedur kemanan informasi harus dijalankan dari level manajemen hingga pelaksana teknis	untuk mengatur akses informasi ke server agar tidak terjadi hal-hal yang merugikan RRI Surabaya.
2.	Terdapat kepastian manajemen bahwa pengguna memiliki keterampilam yang sesuai kualifikasi	Telah dilakukan pemeriksaan di bagian PMB bahwa pegawai yang menggunakan sistem informasi sudah sesuai bidang yaitu	Referensi.: ISO 27002 8.2.1 Tanggung jawab manajemen. Pernyataan 8.2.1 no.5 Penyebab: Pada bagian PMB RRI Surabaya tidak	Tanggapan: Pelatihan mengenai keamanan teknologi informasi sudah sering direkomendsikan oleh RRI Sby namun terkendala dana dari RRI Pusat yang tidak menyetujui sehingga karyawan

Tabel 4.31 (Lanjutan)

TEMUAN AUDIT KEAMANAN INFORMASI				Auditor : Dewangga Putra S. Auditee : GILANG SETIO NUGROHO NIP : 19890522 201301 NO1
ASPEK : KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)				Tanggal : 22 Mar-09 Apr 2016 Tanda Tangan :
No	Pernyataan	Temuan	Referensi, Penyebab, Risiko dan Rekomendasi	Tanggapan dan Komitmen Penyelesaian
		dengan cara melakukan pelatihan kepada pegawai. Training dilakukan hanya sekali saja dan belum cukup untuk kondisi saat ini.	ada pelatihan yang berkelanjutan mengenai keamanan informasi. Risiko: Pelatihan penggunaan dan keamanan teknologi informasi yang tidak berkelanjutan akan menyebabkan turunya pengetahuan karyawan terhadap keamanan dan teknologi informasi yang berdampak pada menurunya produktifitas karyawan terhadap instansi penyiaran publik RRI Surabaya. Rekomendasi: a. Pihak Kepala seksi dapat mengajukan pelatihan ke RRI Pusat secara berkelanjutan minimal enam	hanya sebatas otodidag saja mengenai teknologi informasi. Penyelesaian: Pihak kepala seksi bagian PMB selalu mengirimkan surat untuk pelatihan mengenai keamanan teknologi informasi kepada kepala bagian agar diadakan pelatihan mengingat pentingya hal ini, namun menunggu kebijakan dari RRI Pusat.

Tabel 4.31 (Lanjutan)

TEMUAN AUDIT KEAMANAN INFORMASI				Auditor : Dewangga Putra S. Auditee : GILANG SETIO NUGROHO NIP : 19890522 201301 NO1
ASPEK : KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)				Tanggal : 22 Mar-09 Apr 2016 Tanda Tangan :
No	Pernyataan	Temuan	Referensi, Penyebab, Risiko dan Rekomendasi	Tanggapan dan Komitmen Penyelesaian
			bulan sekali. b. Pihak kepala seksi memberikan arahan teknis kepada operasional untuk memperlancar jalanya siaran. c. Bagian operasional menjalankan perintah sesuai instruksi kepala seksi secara bertanggung jawab.	
3.	Terdapat pelatihan kesadaran pentingnya keamanan informasi kepada seluruh pegawai.	Tidak adanya pelatihan mengenai pentingnya kesadaran keamanan informasi pada pengguna/pegawai. Tidak adanya dokumen mengenai pelatihan kesadaran akan keamanan	Ref.: ISO 27002 8.2.2 Pendidikan dan pelatihan keamanan informasi. Pernyataan 8.2.2 no.1 Penyebab: Belum adanya pelatihan mengenai kesadaran keamanan informasi di RRI Sby karena kebijakan dari pusat.	Tanggapan: Dari banyaknya karyawan RRI Sby yang umurnya sudah tua dan minimnya pelatihan mengenai keamanan informasi menjadikan kendala serius dalam menjaga informasi, sehingga hanya kepercayaan antar karyawan saja yang diandalkan selama ini.

Tabel 4.31 (Lanjutan)

TEMUAN AUDIT KEAMANAN INFORMASI				Auditor : Dewangga Putra S. Auditee : GILANG SETIO NUGROHO NIP : 19890522 201301 NO1
ASPEK : KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)				Tanggal : 22 Mar-09 Apr 2016 Tanda Tangan :
No	Pernyataan	Temuan	Referensi, Penyebab, Risiko dan Rekomendasi	Tanggapan dan Komitmen Penyelesaian
		infrormasi, mengenai kesadaran akan keamanan informasi hanya sebatas pemberitahuan lisan.	Risiko: Minimnya kesadaran keamanan informasi bagi karyawan RRI Sby dikawatirkan akan terjadi peretasan server sehingga terjadi kebocoran informasi jatuh ketangan yang tidak bertanggung jawab dan menyebabkan kerugian dipihak RRI Sby. Rekomendasi: a. Bagian kepala seksi dapat mendefinisikan secara teknis jenis pelatihan tentang kesadaran keamanan informasi. b. Prosedur teknis harus dijalankan oleh bagian operasional secara berkelanjutan dan bertanggung	Penyelesaian: Administrator PMB akan lebih serius dalam menanggapi permintaan berita dan arus berita agar terjaganya informasi ketangan yang benar serta menjaga keutuhan berita sampai di meja penyiar.

Tabel 4.31 (Lanjutan)

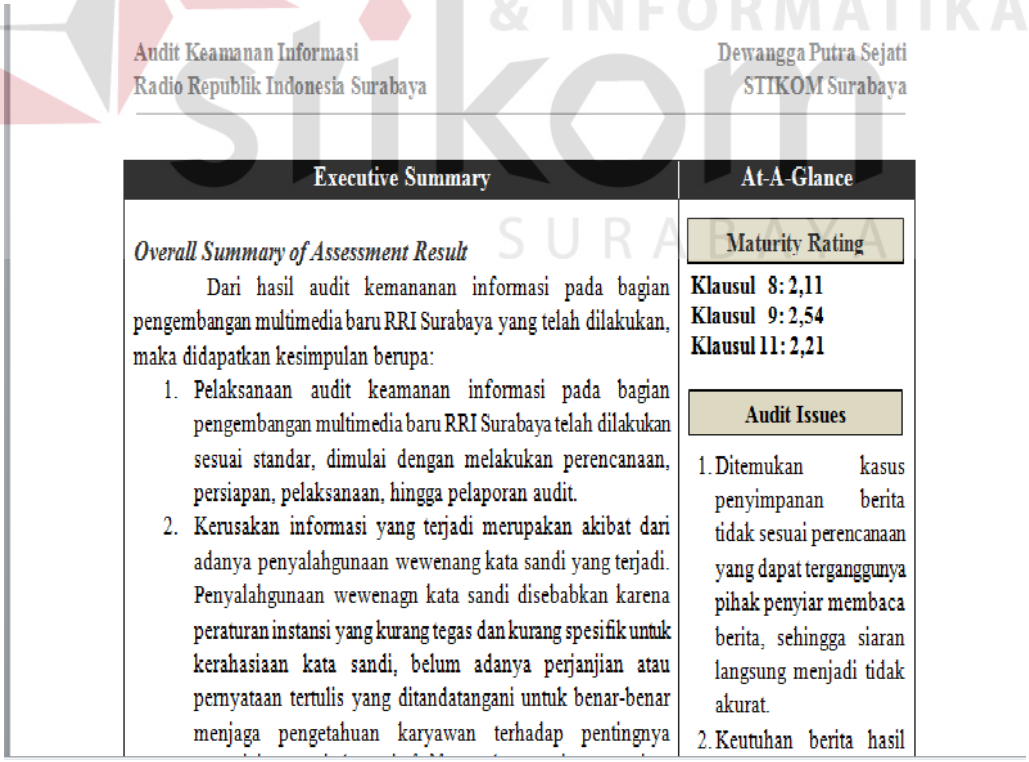
TEMUAN AUDIT KEAMANAN INFORMASI				Auditor : Dewangga Putra S. Auditee : GILANG SETIO NUGROHO NIP : 19890522 201301 NO1
ASPEK : KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)				Tanggal : 22 Mar-09 Apr 2016 Tanda Tangan :
No	Pernyataan	Temuan	Referensi, Penyebab, Risiko dan Rekomendasi	Tanggapan dan Komitmen Penyelesaian
			jawab. c. Bagian operasional menjalankan prosedur keamanan informasi dengan bertanggung jawab dan membuat log harian mengenai tugas yang diselesaikan.	

Dari hasil wawancara dengan pihak PMB dan bukti foto maka didapatkan temuan pada klausul 8 (Delapan) Keamanan Sumber Daya Manusia dengan obyek kontrol 8.2.1 pernyataan no.2 tentang tanggung jawab manajemen yaitu adanya karyawan yang belum mengerti prosedur sebelum mengakses data ke ruang penyimpanan informasi, pelatihan karyawan tentang pemrosesan informasi masih kurang memadai. Pada obyek kontrol 8.2.2 pernyataan no.1 tentang pendidikan dan pelatihan keamanan informasi yaitu tidak adanya kesadaran pentingnya keamanan informasi kepada pengguna/pegawai. Untuk klausul 9 (Sembilan) Keamanan Fisik dan Lingkungan dengan obyek kontrol 9.1.2 pernyataan no.3 yaitu Kontol masuk fisik yaitu tidak dipakainya kartu pengenal oleh masing masing karyawan, pada obyek kontrol 9.2.3 pernyataan no.1 tentang Keamanan pengkabelan yaitu masih adanya kabel yang belum dirapikan. Temuan pada klausul 11 Kontrol akses dengan obyek kontrol 11.1.1 pernyataan no.1 tentang kebijakan kontrol akses yaitu tidak adanya dokumen yang mengatur tentang kebijakan penyimpanan informasi, pada obyek kontrol 11.2.3 pernyataan no. 2 dan 3 tentang Manajemen kata sandi pengguna hanya terdapat pernyataan lisan untuk menjaga kata sandi dan tidak ada sanksi apabila melanggar serta tidak ada dokumen yang mengatur menjaga kerahasiaan kata sandi. Dari hasil temuan yang didapatkan maka rekomendasi yang dapat diberikan adalah adanya dokumen yang mengatur mengenai pentingnya prosedur keamanan informasi sebelum mengakses data informasi dan tertulis dalam tugas pokok dan fungsi (TUPOKSI), segera dilakukan pelatihan kesadaran keamanan informasi yang terdokumentasi mengenai pelatihan tersebut, memakai kartu pengenal sesuai standar yang diterapkan oleh instansi agar memudahkan identifikasi setiap pemakainya, segera

membuat dokumen yang mengatur tentang kebijakan penyampaian informasi dan memberitahukan kepada bagian terkait yang berhubungan dengan bagian PMB agar terjaganya fasilitas penyimpanan informasi di RRI Sby, menerapkan sanksi dan peringatan serta dokumentasi untuk menjaga kata sandi sangat perlu diterapkan guna mengurangi risiko kehilangan data informasi dalam *server*.

4.4 Hasil Pelaporan Audit

Setelah dilakukan penyusunan draft laporan audit keamanan sistem informasi berupa kertas kerja audit, temuan dan tanggapan *auditee* sebagai bentuk tanggung jawab atas penugasan audit keamanan informasi yang telah selesai dilaksanakan maka dilakukan persetujuan audit. Hasil persetujuan draft laporan audit dapat dilihat pada Gambar 4.9 dan selengkapnya dapat dilihat pada Lampiran 11.



Audit Keamanan Informasi
Radio Republik Indonesia Surabaya

Dewangga Putra Sejati
STIKOM Surabaya

Executive Summary	At-A-Glance
Overall Summary of Assessment Result Dari hasil audit kemananan 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	**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. Keutuhan berita hasil

Gambar 4.10 Laporan audit keamanan informasi