EVALUASI KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI PADA KANTOR WILAYAH DITJEN PERBENDAHARAAN NEGARA JAWA TIMUR

Mustaqim Siga[1)], Tony Dwi Susanto[2)], Bekti Cahyo Hidayanto[3)]
Jurusan Sistem Informasi, Fakultas Teknologi Informatika
Institut Teknologi Sepuluh Nopember (ITS)
Jl. Arief Rahman Hakim, Surabaya, 60111
Telp : (031) 5999944, Fax : (031) 5964965
E-mail : mustaqim.siga11@mhs.is.its.ac.id[1)], tonydwisusanto@is.its.ac.id[2)], bekticahyo@is.its.ac.id[3)]

Abstrak

Hadirnya KMK No. 479/KMK.01/2010 sebagai kebijakan dan standar 478arrin manajemen keamanan informasi (SMKI) di lingkungan Kementerian Keuangan menjadikannya sebagai pedoman dalam rangka melindungi 478arri informasi Kementerian Keuangan dari berbagai bentuk ancaman baik dari dalam maupun luar lingkungan Kementerian Keuangan. Selanjutnya, hal yang paling penting di dalam pelaksanaan Sistem Manajemen Keamanan Informasi (SMKI) adalah melakukan evaluasi terhadap pelaksanaan SMKI yang diistilahkan monitor and review. Evaluasi diperlukan dalam rangka menjamin pelaksanaan SMKI agar 478arring-kontrol keamanan yang dipilih mampu melindungi 478arri informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi institusi. Evaluasi pada penelitian ini dilakukan dengan menggunakan Indeks KAMI yang disusun oleh Kementerian Komunikasi dan Informatika. Indeks KAMI adalah alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di instansi pemerintah. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2005. Hasil dari penelitian ini adalah evaluasi untuk mendapatkan penilaian mengenai pengelolaan keamanan TI, mengetahui tingkat kematangan pengelolaan keamanan teknologi informasi dan mendapatkan rekomendasi atas hasil analisis pengelolaan keamanan informasi.

Kata kunci: *evaluasi, keamanan informasi, indeks KAMI*

Abstract

Presence of KMK No.479/KMK.01/2010 as a policy and standard information security management system (ISMS) in Ministry of Finance make into guidelines to protect Ministry of Finance information assets from every inside and outside threats. Next, the most important of information security management (ISMS) implementation are evaluations for ISMS implementation called monitor and review. Evaluation needed to ensure security controls that been choosing could protect information assets from every risks and have good security confidence level for institution. In this research, evaluation of information security management using KAMI Index arranged by Ministry of Communication and Information. KAMI Index is evaluation instruments to analyze information security level at government institution. Evaluation conducted to areas that being scope of research that comply for every aspect defined by ISO/IEC 27001:2005. Outcome of this research is evaluation to get results of IT security management level, understanding about maturity level of IT security management and recommendations based on analysis result of information security management.

Keywords: *evaluation, information security, KAMI Index*

1. PENDAHULUAN

Kehadiran KMK No. 479/KMK.01/2010 tentang Kebijakan dan Standar Sistem Manajemen Keamanan Informasi (SMKI) di lingkungan Kementerian Keuangan merupakan wujud pelaksanaan Rencana Strategis Kementerian Keuangan Tahun 2010-2014 Nomor. 40/KMK.01/2010 terkait keamanan teknologi informasi (ITSM). Hal yang paling penting di dalam pelaksanaan Sistem Manajemen Keamanan Informasi (SMKI) adalah melakukan evaluasi terhadap pelaksanaan SMKI yang diistilahkan *monitor and review*. Dalam siklus PDCA, evaluasi ini merepresentasikan proses *Check* [1]. Dalam perkembangannya, evaluasi pengelolaan keamanan informasi bagi

penyelenggara pelayanan 479arrin didasarkan pada Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik dengan alat evaluasi berupa penggunaan Indeks Keamanan Informasi (Indeks KAMI). Tujuan utamanya adalah membandingkan seberapa jauh persyaratan klausul-klausul ISO 27001 terkait keamanan informasi telah dipenuhi, baik pada aspek kerangka kerja (kebijakan dan prosedur) maupun aspek penerapannya [2].
Tujuan dari penelitian ini adalah untuk mendapatkan penilaian mengenai pengelolaan keamanan TI pada Kanwil DJPBN Jawa Timur, mengetahui tingkat kematangan pengelolaan keamanan TI dan mendapatkan rekomendasi berdasarkan hasil analisis pengelolaan keamanan informasi pada Kanwil DJPBN Jawa Timur.

2. TINJAUAN PUSTAKA

Pada bagian ini ada 2 (dua) uraian berkaitan dengan Kantor Wilayah Direktorat Jenderal Perbendaharaan Jawa Timur sebagai obyek penelitian dan Indeks Keamanan Informasi sebagai alat evaluasi pelaksanaan keamanan informasi.

2.1 Kantor Wilayah Ditjen Perbendaharaan Negara Jawa Timur

Kantor Wilayah Direktorat Jenderal Perbendaharaan (Kanwil Ditjen Perbendaharaan) adalah unit eselon II secara vertikal di bawah Direktorat Jenderal Perbendaharaan dalam struktur organisasi pada Kementerian Keuangan.. Hal ini terkait erat dengan pelaksanaan reformasi organisasi dan menajamen keuangan negara dan sebagai upaya menyelaraskan perangkat organisasi melalui penegasan fungsi Kementerian Keuangan atas amanat dari UU Nomor 17 Tahun 2003 tentang Keuangan Negara dan UU Nomor 1 Tahun 2004 tentang Perbendaharaan Negara
Tugas Kanwil Ditjen Perbendaharaan Provinsi Jawa Timur adalah melaksanakan koordinasi, pembinaan, penyuluhan, bimbingan teknis, penelaahan, monitoring, evaluasi, penyusunan laporan, verifikasi dan pertanggungjawaban di bidang perbendaharaan dalam wilayah kerja Provinsi Jawa Timur berdasarkan peraturan perundang-undangan yang berlaku.

2.2 Indeks Keamanan Informasi

Indeks KAMI adalah alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di instansi pemerintah. Alat evaluasi ini tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi. Bentuk evaluasi yang diterapkan dalam indeks KAMI dirancang untuk dapat digunakan oleh instansi pemerintah dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan TIK dalam mendukung terlaksananya Tugas Pokok dan Fungsi yang ada. Penggunaan dan publikasi hasil evaluasi Indeks KAMI merupakan bentuk tanggungjawab penggunaan dana publik sekaligus menjadi sarana untuk meningkatkan kesadaran mengenai kebutuhan keamanan informasi di instansi pemerintah. Evaluasi ini dianjurkan untuk dilakukan oleh pejabat yang secara langsung bertanggung jawab dan berwenang untuk mengelola keamanan informasi di seluruh cakupan instansinya.

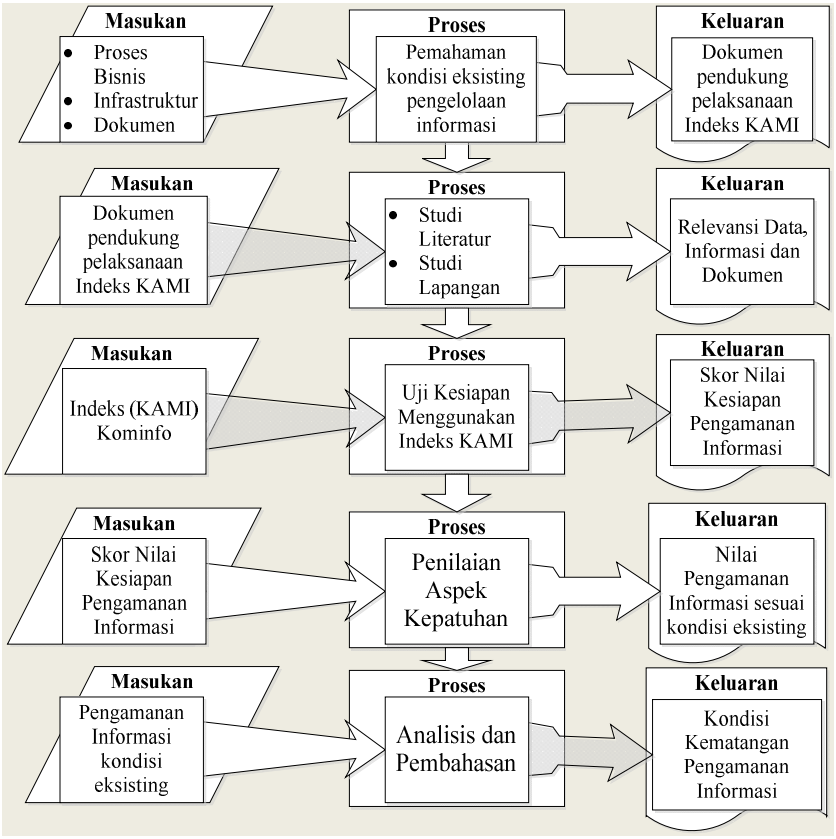
Untuk implementasinya, indeks KAMI bagi Penyelenggara Pelayanan Publik meliputi 5 (lima) area, sebagai berikut:

1. Kebijakan dan manajemen organisasi, terkait dengan program kerja yang berkesinambungan, alokasi anggaran, evaluasi program dan strategi peningkatan kinerja tata kelola keamanan informasi;
2. Manajemen risiko, terkait dengan kerangka kerja pengelolaan risiko dengan definisi yang eksplisit terkait ambang batas diterimanya risiko, program pengelolaan risiko dan langkah mitigasi;
3. Kerangka kerja, terkait dengan sejumlah kebijakan dan prosedur kerja operasional, termasuk strategi penerapan, pengukuran efektifitas 479arring dan langkah perbaikan;
4. Manajemen aset informasi, terkait dengan keberadaan 479arri informasi, termasuk keseluruhan proses yang bersifat teknis maupun 479arring479rative dalam siklus penggunaan 479arri tersebut.;
5. Teknologi dan keamanan informasi, terkait dengan area mensyaratkan adanya strategi teknologi yang terkait dengan tingkatan risiko.

Detail bentuk pengamanan yang dibahas di masing-masing area dapat dipahami dari 119 pertanyaan (kajian mandiri) yang disediakan dalam lima area tersebut.

3. METODOLOGI

Metodologi pengerjaan penelitian ini secara garis besar terdiri atas tahapan-tahapan berikut.



Gambar 1. Metodologi Evaluasi dengan Indeks KAMI

4. PEMBAHASAN

Pada bagian ini akan dibahas mengenai hasil perbandingan penilaian aspek kepatuhan, hasil kondisi peran TIK, dan hasil status kesiapan keamanan informasi pada Kanwil DJPBN Jawa Timur.

4.1 Penilaian Aspek Kepatuhan

Penilaian Aspek Kepatuhan dilakukan terinci dengan menganalisis isian item pertanyaan pada Indeks KAMI, item temuan berdasarkan kondisi eksisting, bukti kesesuaiannya serta catatan. Penghitungan komparasi sederhana antara *self assestment* (penilaian secara personal oleh institusi) dan *objective assestment,* (penilaian yang dilaksanakan berdasarkan bukti dan temuan) dapat terlihat sebagai berikut:

Tabel 1. Perbandingan Aspek Kepatuhan

Area	*Self Assestment*	*Objective Assestment*
Peran TIK	40	36
Nilai 5 Area	423	337

Berikut ini perbandingan porsentase Aspek Kepatuhan:

Tabel 2. Porsentase Perbandingan Kepatuhan

	Self Assestment	*Objective Assestment*
Nilai	$\frac{423 \times 100\%}{588} = 72\%$	$\frac{337 \times 100\%}{588} = 57.31\%$

- Perhitungan didapat dengan membandingkan antara nilai sekarang dengan nilai maksimal status kesiapan dengan peran TIK tinggi yaitu 588.
- Nilai perbandingan kondisi *self assestment* cenderung lebih tinggi karena belum dilakukan penilaian aspek kepatuhan terhadap semua bukti pendukung evaluasi keamanan informasi. Sedangkan untuk kondisi

setelahnya sudah dilakukan penilaian aspek kepatuhan untuk mengetahui apakah isian responden sesuai dengan ketersediaan bukti atau tidak.

- Hasil perbandingan tersebut menjelaskan mengenai kondisi ketersediaan perangkat keamanan informasi baik secara SDM, dokumentasi, hingga tindakan teknikal yang yang sudah dilakukan namun perlu diperbaiki dalam hal kelengkapan serta ketersediaan.

4.2 Hasil Kondisi Peran TIK

Dari hasil penelitian, terlihat nilai alokasi anggaran tahunan terkait dengan TIK dibawah 1 Milyar dan pengguna yang dalam hal ini dimaksudkan adalah karyawan Kanwil DJPBN juga menunjukkan angka yang rendah berkisar pada 115 pegawai. Namun disisi peran dan fungsinya menunjukkan bahwa tingkat ketergantungan Kanwil DJPBN Jawa Timur akan kebutuhan TIK bernilai tinggi yang secara ringkas dapat dilihat di 481arri bawah ini:

Tabel 3. Kondisi Peran TIK.

Status Ketergantungan		
Terendah	Tertinggi	Klasifikasi
0	12	Rendah
13	24	Sedang
25	36	**Tinggi**
37	48	Kritis

Jika secara menyeluruh dilihat dari status ketergantungan yang bersifat tinggi, maka dampak kerugian terkait keamanan informasi dapat menghambat proses perbendaharaan dan penganggaran baik secara data atau informasi.

4.3 Hasil Status Kesiapan Keamanan Informasi

Pada bagian ini akan dibahas mengenai hasil skor akhir secara keseluruhan lima area keamanan informasi yang dikelola oleh Kantor Wilayah Direktorat Jenderal Perbendaharaan Jawa Timur. Berikut hasil Tingkat Kematangan untuk seluruh area berdasarkan tingkat validitas skor pada *objective assestment* dalam penelitian ini:

Tabel 4. Status Kematangan 5 Area

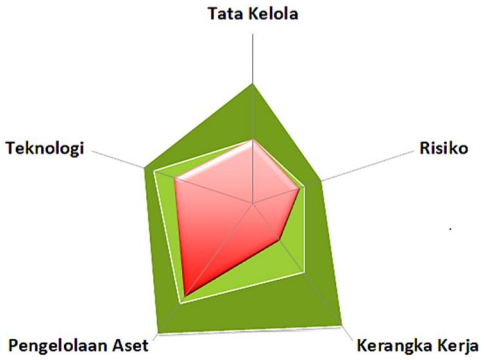
Validitas	Tata Kelola	Pengelolaan Risiko	Kerangka Kerja	Pengelolaan Aset	Teknologi
Tingkat Kematangan I					
Validitas	Yes	Yes	Yes	Yes	Yes
Status	I	I	I	I	I
Tingkat Kematangan II					
Validitas	Yes	Yes	Yes	Yes	Yes
Status	II	II	II	II	II
Tingkat Kematangan III					
Validitas	No	No	No	No	No
Status	No	No	No	No	II
Tingkat Kematangan IV					
Validitas	No	No	No	No	No
Status	No	No	No	No	No
Status Akhir	II	II	II	II	II

Dari hasil penelitian berdasarkan *objective assessment* di atas dapat dilihat bahwa perolehan nilai Tingkat Kematangan merata pada perolehan skor keseluruhan yang terdapat di semua area pengamanan informasi (TK) yaitu pada level II. Level II dalam indeks KAMI merepresentasikan kondisi terkini mencakup 5 area pengelolaan keamanan informasi pada Kanwil DJPBN Jawa Timur di antaranya:

a. Pengamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.
b. Proses pengamanan berjalan tanpa dokumentasi atau rekaman resmi. Beberapa tindakan pengamanan telah memiliki kebijakan setingkat PMK ataupun KMK namun belum di*cascade* ke dalam prosedur atau panduan yang implementatif pada pelaksanaan pengamanan informasi di tingkat operasional / pelaksana.
c. Bentuk pengamanan secara keseluruhan belum dapat dibuktikan efektivitasnya. Hal ini terlihat dari belum adanya laporan / *report* dari seluruh langkah pengamanan yang dilakukan.
d. Kelemahan dalam manajemen pengamanan masih banyak ditemukan dan tidak dapat diselesaikan dengan tuntas oleh pelaksana maupun pimpinan sehingga menyebabkan dampak yang sangat signifikan.
e. Manajemen pengamanan belum mendapatkan prioritas dan tidak berjalan secara konsisten. Hal ini terlihat dari serangkaian kegiatan pengamanan yang pelaksanannya belum menjadi bagian dari SFO dan ketiadaan dokumentasi yang runtut dari proses identifikasi, analisis, implementasi, evaluasi dan pelaporan.

f. Pihak yang terlibat kemungkinan besar masih belum memahami tanggung jawab mereka (berdasarkan Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik).

Hasil keseluruhan terhadap lima area indeks KAMI ditampilkan pada diagram jaring laba-laba skor Indeks KAMI di bawah ini:



Gambar 2. Diagram 482arring Indeks KAMI

Warna merah responden menjelaskan mengenai persebaran jawaban dari lima area :

- Level kepatuhan paling signifikan didapat Pengelolaan Aset karena telah melampaui atau memenuhi bagian Kerangka Kerja Dasar atau Tingkat Kematangan II menuju Tingkat Keamanan II+ (selisih valid 3 poin).
- Sedangkan area lainnya yakni Tata Kelola, Pengelolaan Risiko, Kerangka Kerja dan Teknologi dinyatakan butuh peningkatan karena jawaban responden terhadap Kerangka Kerja hanya pada Tingkat Kematangan II.
- Untuk menuju pada jaring Kepatuhan ISO 27001/SNI yang lebih baik maka Kanwil DJPBN Jawa Timur harus memperhatikan semua area baik aspek kerangka kerja dasar, konsistensi penerapan dan tindakan peningkatan kinerja keamanan.

Dari aspek peran TIK, Kanwil DJPBN Jawa Timur menunjukkan skor sangat tinggi yaitu 36 dari 48. Sedangkan status kesiapan pada skor 337 dari nilai maksimal 588 yang artinya masih perlu perbaikan untuk kelengkapan perangkat keamanan seluruh area pengelolaan keamanan informasi.

Tabel 5. Status Kesiapan Keamanan Informasi Keseluruhan

Skor	Range		Status
25-36	0	272	Tidak Layak
	273	392	Perlu Perbaikan
	393	588	Baik/Cukup

Langkah-langkah perbaikan pengelolaan keamanan informasi Kanwil DJPBN Jawa Timur diantaranya :

1. Melaksanakan dan menerapkan semua kebijakan dan prosedur keamanan informasi pada semua area pengamanan.
2. Memonitoring segala aktivitas teknologi informasi meliputi kinerja pegawai, kinerja hardware, kinerja software, dan pengimplementasian penerapan regulasi terkait pengelolaan keamanan informasi.
3. Mengevaluasi setiap penerapan kebijakan dan prosedur terkait keamanan informasi untuk menilai efektifitas dan efisiensi kinerja terhadap segala aktivitas teknologi informasi (berdasarkan KMK No.479/KMK.01/2010, KMK No.512/KMK.01/2009, KMK No.21/KMK.01/2012, dll)

5. KESIMPULAN DAN REKOMENDASI

Pada bagian ini menjelaskan kesimpulan dan rekomendasi untuk pengelolaan keamanan informasi pada Kantor Wilayah DJPBN Jawa Timur.

5.1 Kesimpulan

Kesimpulan yang dapat diambil secara menyeluruh dalam pengerjaan penelitian dengan studi kasus evaluasi pengelolaan keamanan perbendaharaan negara oleh Kanwil DJPBN Jawa Timur antara lain :

6. Dari aspek penilaian peran TIK bagi Kanwil DJPBN menunjukkan angka relatif tinggi yang menandakan peran vital TIK bagi pelaksananaan perbendaharaan (skor 36 dari 48).
7. Status kesiapan pengelolaan keamanan informasi yang meliputi kelengkapan perangkat keamanan pada 5 (lima) area dinilai masih perlu adanya perbaikan (skor 337 dari nilai maksimal 588).

8. Hasil penilaian berdasarkan aspek kepatuhan menunjukkan pengelolaan keamanan informasi pada Kanwil DJPBN Jawa Timur sudah dalam penerapan, namun dinilai masih perlu diperbaiki dalam hal kelengkapan perangkat pengamanannya (prosentase 57,31% temuan sesuai dan 14.69 % temuan yang tidak sesuai).
9. Tingkat kematangan seluruh area berada pada level II dari level V yang artinya terdapat pemahaman keamanan informasi di Kanwil DJPBN Jawa Timur namun masih tergolong aktif bukan proaktif.

5.2 Rekomendasi

5.2.1 Rekomendasi Area Tata Kelola Keamanan Informasi

a. Memperbaiki beberapa kelemahan dalam sistem manajemen tata kelola sehingga dapat menghasilkan dampak signifikan terhadap pengelolaan keamanan informasi
b. Meningkatkan kesadaran semua pihak baik pimpinan, pelaksana dan pihak ketiga untuk menyadari tanggungjawab pengelolaan keamanan informasi
c. Menerapkan seluruh persyaratan dan standar kompetensi dan keahlian pelaksana dalam pengelolaan keamanan informasi
(berdasarkan KMK No.479/KMK.01/2010 Poin I, II, IV)

5.2.2 Rekomendasi Area Pengelolaan Risiko

a. Merencanakan dan menerapkan seluruh pengelolaan risiko menjadi bagian dari kriteria penilaian efektifitas pengamanan terhadap semua layanan perbendaharaan Kanwil DJPBN
b. Merencanakan dan mengevaluasi secara menyeluruh terhadap program pengelolaan risiko keamanan informasi yang akan dilaksanakan
c. Melaksanakan dokumentasi peningkatan langkah mitigasi yang diterapkan untuk mengetahui kondisi perkembangan penanganan dan pengendalian risiko
(berdasarkan PMK No.191/PMK.09/2008 dan KMK No.479/KMK.01/2010 Poin III, V dan XI)

5.2.3 Rekomendasi Area Kerangka Kerja Keamanan Informasi

a. Merencanakan dan menerapkan kebijakan dan prosedur keamanan informasi terhadap semua aktifitas teknologi informasi yang sudah didefinisikan komposisi, peran, wewenang dan tanggungjawabnya
b. Merencanakan dan menerapkan proses pengembangan rencana pemulihan bencana layanan TIK.
c. Merencanakan evaluasi pengelolaan kebijakan keamanan informasi yang telah digunakan dengan mencantumkan peran, wewenang dan tanggungjawabnya
(berdasarkan KMK No.479/KMK.01/2010 dan KMK No.260/KMK.01/2009)

5.2.4 Rekomendasi Area Pengelolaan Aset Keamanan Informasi

a. Merencanakan dan menerapkan secara menyeluruh proses penerapan definisi tingkatan akses dan matrix yang merekam alokasi akses
b. Merencanakan dan melaksanakan secara menyeluruh tata tertib pengamanan komputer, email, intranet dan internet serta pertukaran data dan informasi
c. Melaksanakan pengendalian dan evaluasi secara menyeluruh terhadap aset informasi dan dokumentasi terhadap semua aktifitas pengelolaan keamanan aset informasi
(berdasarkan KMK No.479/KMK.01/2010 Poin III dan VIII, KMK No.512/KMK.01/2009 dan KMK No.21/KMK.01/2012)

5.2.5 Rekomendasi Area Teknologi dan Keamanan Informasi

a. Merencanakan penerapan secara menyeluruh pada proses konfigurasi standar untuk keamanan sistem bagi keseluruhan asset informasi dan perangkat jaringan yang dimutakhirkan
b. Melaksanakan secara menyeluruh dokumentasi dan pelaporan terhadap segala aktifitas pengelolaan TIK (berdasarkan KMK No.479/KMK.01/2010, KMK No. 512/KMK.01/2009, KMK No. 274/KMK.01/2010)

6. DAFTAR RUJUKAN

[1] Sarno, R., 2009. *Sistem Manajemen Keamanan Informasi*. Surabaya : ITS Press.

[2] Ditkaminfo., 2011. *Panduan Penerapan Tata Kelola Teknologi Informasi Bagi Penyelenggara Pelayanan Publik*. Jakarta : Ditjen Aptika Kominfo