SAINSTEK : JURNAL SAINS DAN TEKNOLOGI
Penerbit: AMSET IAIN Batusangkar dan IAIN Batusangkar Press
Website: http://ecampus.iainbatusangkar.ac.id/ojs/index.php/sainstek
E-mail: sainstek@iainbatusangkar.ac.id

Desember 2020
Vol 12 No 2
ISSN: 2085-8019 (p)
ISSN: 2580-278X (e)
pp : 71-78

Evaluasi Internal Keamanan Informasi pada Dinas Komunikasi dan Informatika Kota Palembang

Ilham Bintang[1], Catur Eri Gunawan[1*], Freddy Kurnia Wijaya[1]

[1]Sistem Informasi, Universitas Islam Negeri Raden Fatah Palembang
Jalan Prof. K. H. Zainal Abidin KM. 3.5, Kota Palembang, Sumatera Selatan, Indonesia
**email: caturerig@radenfatah.ac.id*

Article History
Received: 7 November 2020
Reviewed: 23 November 2020
Published: 31 Desember 2020

Key Words
Information Security;
Government Agencies;
Maturity Level;
Completeness of Information Security.

Abstract
This article aims to provide an overview of the conditions of readiness (completeness and maturity) of information security at Diskominfo Palembang which is carried out internally. The research instrument used was a questionnaire taken from the guidelines of Indeks KAMI version 3.1. The research method used in this article is descriptive quantitative. The answers for each area are collected, then with the calculations that have been available in the guidelines of Indeks KAMI version 3.1, the results will be obtained from the completeness of the work program that has been carried out and the maturity level of information security at Diskominfo Palembang. The assessment result of the completeness of the information security work program is 338, based on the provisions of Indeks KAMI, so this means that the readiness status of Diskominfo Palembang still needs improvement. Meanwhile, the assessment of the maturity level of information security at Diskominfo Palembang is at level I-II. This means that the maturity level of information security is still in its initial condition and is implementing an information security framework in the activities of using information technology.

PENDAHULUAN

Teknologi informasi telah mengalami perkembangan yang pesat (Gunawan, 2020) dan juga menawarkan kemudahan dalam berkomunikasi, penyebaran informasi (Gunawan et al., 2013), dan pengolahan data. Aset-aset organisasi pun saat ini telah bertambah, tidak hanya mengenai perangkat perkantoran dan dokumentasi instansi tetapi juga informasi yang dihasilkan dari berbagai perangkat lunak yang digunakan oleh instansi dalam upaya mempermudah pemberian pelayanan kepada masyarakat. Penggunaan teknologi informasi ini pun tentunya membutuhkan manajemen keamanan informasi untuk menjaga aset-aset instansi tersebut (Gunawan & Fenando, 2018).

Dinas Komunikasi dan Informatika (Diskominfo) Kota Palembang yang merupakan penyelenggara urusan pemerintah bidang komunikasi dan informatika Kota Palembang tentunya perlu menerapkan manajemen keamanan informasi. Dari hasil wawancara dengan pihak Teknologi Informasi (TI) Diskominfo Kota Palembang, diketahui bahwa sejak diterapkannya penggunaan teknologi informasi pada tahun 2018 yang menghasilkan berbagai informasi, pihak TI baru satu kali melakukan evaluasi keamanan informasi di lingkungan Diskominfo Kota Palembang. Hal ini tentunya tidak sejalan dengan keinginan pemerintah yang telah menghimbau kepada instansi pemerintah pelayanan publik (Setiawan, 2013), baik pusat maupun daerah untuk

melakukan evaluasi keamanan informasi mandiri *(self assesment)* (Tim Direktorat Keamanan Informasi, 2011) minimal dua kali dalam setahun (Tim Penyusun Indeks KAMI 3.1, 2015). Pada penelitian lainnya yang juga menyebutkan pentingnya untuk melakukan evaluasi keamanan informasi terhadap penggunaan teknologi informasi perlu dilakukan oleh instansi pelayanan publik (Firmana et al., 2013; E. L. Putra et al., 2014; Ridho et al., 2012; Saputra & Gilang, 2016).

Semakin banyaknya informasi yang dihasilkan, maka sangat perlu secara rutin dilakukan evaluasi keamanan informasi di suatu instansi guna mencegah risiko keamanan informasi (Rahardjo, 2017). Dalam penelitian ini digunakan Indeks Keamanan Informasi (KAMI) versi 3.1. Indeks KAMI merupakan alat evaluasi yang digunakan untuk menganalisa tingkat kesiapan pengamanan informasi di instansi pemerintah. Indeks KAMI dipilih dalam penelitian ini dikarenakan sangat cocok digunakan untuk instansi pemerintah. Artikel ini bertujuan untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) pengamanan informasi pada Diskominfo Kota Palembang yang dilakukan secara internal. Di dalam pedoman Indeks KAMI, tidak didukung dengan rekomendasi yang berupa praktik terbaik yang harus dilakukan dalam pengelolaan dan pengamanan informasi. Oleh karena itu, di dalam penelitian ini digunakan ISO/IEC 27002:2013.

Hasil evaluasi setiap area yang mendapatkan nilai rendah akan dikumpulkan dan diberikan rekomendasi perbaikan. Rekomendasi perbaikan yang akan diberikan berdasarkan pada ISO/IEC 27002:2013, yang merupakan praktik terbaik dalam pengelolaan keamanan informasi (ISO Members, 2013). Dengan memberikan rekomendasi yang tepat maka risiko keamanan informasi dapat diminimalisir dengan baik. Dari hasil evaluasi internal ini, pihak Diskominfo Palembang dapat mengetahui program kerja untuk pengamanan informasi seperti apa saja yang sebaiknya dilakukan dan diterapkan di lingkungan Diskominfo Palembang.

METODE PENELITIAN

Pada penelitian ini digunakan metode penelitian deskriptif dengan pendekatan kuantitatif. Metode deskriptif kuantitatif digunakan untuk menggambarkan, meninjau, serta menggali informasi (E. A. Putra, 2015) yang mendalam dari hasil penelitian kemudian dituangkan dalam bentuk deskripsi. Penelitian ini juga bersifat mengekplorasi kesesuaian penerapan pengamanan informasi berdasarkan Indeks KAMI versi 3.1 di lingkungan Diskominfo Palembang.

Di dalam artikel ini, untuk melakukan evaluasi penerapan keamanan informasi digunakan Indeks KAMI versi 3.1. Di dalam indeks KAMI ini telah terdapat butir-butir pertanyaan yang digunakan untuk mengevaluasi kelengkapan dan kematangan kerangka kerja keamanan informasi. Berdasarkan indeks KAMI, butir-butir pertanyaan tersebut dibagi sesuai area penilaian yang menjadi target penerapan keamanan informasi.

HASIL DAN PEMBAHASAN

Identifikasi Responden

Pada penelitian ini responden penelitian yang terlibat untuk mengisi butir-butir pertanyaan merupakan pihak-pihak yang memang memegang peranan penting dalam pengelolaan keamanan informasi di Diskominfo Kota Palembang. Terdapat 2 (dua) bagian penting yang dipilih untuk mengisi seluruh butir-butir pertanyaan yang terdapat pada indeks KAMI. Secara ringkas responden penelitian dapat dilihat pada Tabel 1.

Tabel 1. Responden Penelitian

Unit	Jumlah
Teknologi Informasi dan Persandian	3
Pengelolaan *E-Government*	3
Total	6

Evaluasi Terhadap Penerapan Keamanan Informasi

Di dalam indeks KAMI terdapat beberapa area yang menjadi target penilaian penerapan keamanan informasi, yaitu: (1) kategori Sistem Elektronik yang digunakan oleh instansi, (2) Tata Kelola Keamanan Informasi, (3) Pengelolaan Risiko Keamanan Informasi, (4) Kerangka Kerja Keamanan Informasi, (5) Pengelolaan Aset Informasi, (6) Teknologi dan Keamanan Informasi.

Perhitungan pada Indeks KAMI sudah tercantum pada file dengan format *Microsoft Excel* yang merupakan pedoman pelaksanaan Indeks KAMI, sehingga seluruh hasil perhitungan yang didapat sudah mengikuti pedoman Indeks KAMI. Berikut ini akan ditampilkan hasil perhitungan yang telah dilakukan, kemudian pada bagian pembahasan akan dijelaskan makna dari setiap perhitungan yang telah didapatkan.

Area 1: Kategori Sistem Elektronik

Tahap pertama dalam indeks KAMI yaitu dengan mengevaluasi sistem elektronik yang digunakan. Tahap ini harus dilakukan paling awal sebelum masuk ke area lainnya. Pihak dari Diskominfo Kota Palembang harus mampu mendefinisikan seberapa besar lingkup dari penggunaan Teknologi Informasi dan Komunikasi di lingkungannya. Pada tahap ini, responden diminta untuk mendefinisikan lingkup dari penggunaan Teknologi Informasi dan Komunikasi (TIK) Diskominfo Kota Palembang. Pada area sistem elektronik ini terdapat 10 (sepuluh) pertanyaan, dengan jawaban secara ringkas dapat dilihat pada Tabel 2.

Area 2: Tata Kelola Keamanan Informasi

Pada area tata kelola keamanan informasi terdapat 22 pertanyaan. Untuk perhitungan penilaian area 2 sampai dengan area 6 mengacu pada Tabel 3.

Tabel 2. Skor Area Sistem Elektronik

Status (1)	Skor (2)*	Banyak Jawaban (3)	(2) x (3)
A	5	4	20
B	2	2	4
C	1	4	4
		Total Area 1	28

*Ketentuan dari indeks KAMI

Tabel 3. Acuan Penilaian Area 2 Sampai Area 6

Status Pengaman	Kategori Pengamanan		
	1	2	3
Tidak Dilakukan	0	0	0
Dalam Perencanan	1	2	3
Dalam Penerapan atau Diterapkan Sebagian	2	4	6
Diterapkan secara Menyeluruh	3	6	9

Hasil penilaian pada area tata kelola keamanan informasi secara ringkas dapat dilihat pada Tabel 4.

Tabel 4. Skor Area Tata Kelola Keamanan Informasi

Status	Kategori		
	1	2	3
Tidak dilakukan	2	0	1
Dalam perencanaan	0	0	0
Dalam penerapan/ diterapkan sebagian	2	7	4
Diterapkan secara menyeluruh	4	1	1
Total kategori (sesuai ketentuan Tabel 3)	16	34	33
Total Area 2	83		

Area 3: Pengelolaan Risiko Keamanan Informasi

Pada area pengelolaan risiko keamanan informasi terdapat 16 pertanyaan. Secara ringkas hasil penilaian dapat dilihat pada Tabel 5.

Tabel 5. Skor Area Pengelolaan Risiko Keamanan Informasi

Status	Kategori		
	1	2	3
Tidak dilakukan	0	0	0
Dalam perencanaan	0	0	0
Dalam penerapan/ diterapkan sebagian	8	4	2
Diterapkan secara menyeluruh	2	0	0
Total kategori (sesuai ketentuan Tabel 3)	22	16	12
Total Area 3	50		

Area 4: Kerangka Kerja Keamanan Informasi

Pada area kerangka kerja keamanan informasi terdapat 29 pertanyaan. Secara ringkas hasil penilaian dapat dilihat pada Tabel 6.

Tabel 6. Skor Area Kerangka Kerja Keamanan Informasi

Status	Kategori		
	1	2	3
Tidak dilakukan	0	0	7
Dalam perencanaan	8	10	0
Dalam penerapan/ diterapkan sebagian	4	0	0
Diterapkan secara menyeluruh	0	0	0
Total kategori (sesuai ketentuan Tabel 3)	16	20	0
Total Area 4	36		

Area 5: Pengelolaan Aset Informasi

Pada area pengelolaan aset informasi terdapat 38 pertanyaan. Secara ringkas hasil penilaian dapat dilihat pada Tabel 7.

Tabel 7. Skor Area Pengelolaan Aset Informasi

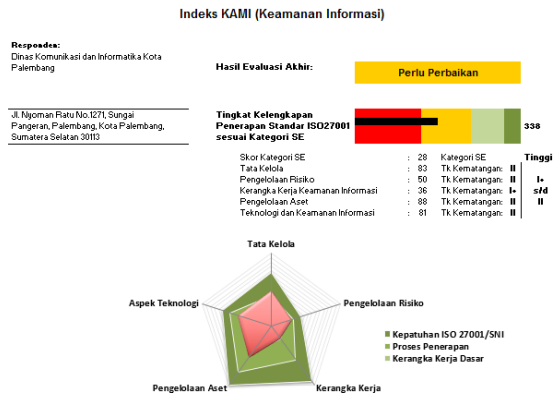
Status	Kategori		
	1	2	3
Tidak dilakukan	3	0	4
Dalam perencanaan	5	0	0
Dalam penerapan/ diterapkan sebagian	9	8	0
Diterapkan secara menyeluruh	7	2	0
Total kategori (sesuai ketentuan Tabel 3)	44	44	0
Total Area 5		88	

Area 6: Teknologi dan Keamanan Informasi

Pada area teknologi dan keamanan informasi terdapat 26 pertanyaan. Secara ringkas hasil penilaian dapat dilihat pada Tabel 8.

Tabel 8. Skor Area Teknologi dan Keamanan Informasi

Status	Kategori		
	1	2	3
Tidak dilakukan	0	0	0
Dalam perencanaan	0	0	1
Dalam penerapan/ diterapkan sebagian	12	9	0
Diterapkan secara menyeluruh	2	2	0
Total kategori (sesuai ketentuan Tabel 3)	30	48	3
Total Area 6		81	



Gambar 1. *Dashboard* Evaluasi Akhir

Pembahasan

Dari hasil penilaian di setiap area yang telah ditentukan di dalam indeks KAMI, maka diperoleh hasil akhir evaluasi mengenai kelengkapan dan kematangan pengelolaan keamanan informasi di Diskominfo Kota Palembang yang dievaluasi secara internal. Dapat dilihat pada Gambar 1.

Dari penilaian ini juga didapat total akhir untuk penilaian kelengkapan pengamanan informasi di lingkungan Diskominfo Kota Palembang sebesar 338. Selain itu, untuk penilaian tingkat kematangan pengamanan informasi di lingkungan Diskominfo Kota Palembang berada pada tingkat I-II.

Penilaian kelengkapan pada indeks KAMI ini mengacu pada ketentuan Tabel 9.

Tabel 9. Acuan Penentuan Status Kesiapan Pengamanan Informasi

Kategori Sistem Elektronik				
Rendah		Skor Akhir		Status Kesiapan
10	15	0	174	Tidak Layak
		175	312	Perlu Perbaikan
		313	535	Cukup
		536	645	Baik
Tinggi		Skor Akhir		Status Kesiapan
16	34	0	272	Tidak Layak
		273	455	Perlu Perbaikan
		456	583	Cukup
		584	645	Baik
Strategis		Skor Akhir		Status Kesiapan
35	50	0	333	Tidak Layak
		334	535	Perlu Perbaikan
		536	609	Cukup
		610	645	Baik

Area Kategori Sistem Elektronik

Pada kategori sistem elektronik ini, nilai yang didapat sebesar 28. Hal ini berarti penggunaan sistem elektronik di lingkungan Diskominfo Kota Palembang sudah menjadi bagian yang sangat penting dan memiliki ketergantungan yang tinggi. Oleh karena itu, pengelolaan keamanan informasi sudah harus diterapkan guna keberlangsungan dan kelancaran ketersediaan akses ke sistem elektronik.

Area Tata Kelola Keamanan Informasi

Pada tata kelola keamanan informasi, nilai yang didapat sebesar 83 dari total 126 (65.87%). Dilihat dari jawaban dan kondisi yang ada terdapat beberapa hal yang tidak dilakukan, yaitu: (1) Pimpinan instansi secara prinsip dan resmi tidak melakukan program pengamanan informasi, termasuk penetapan kebijakan keamanan informasi; (2) Instansi tidak mendefinisikan persyaratan kompetensi dan keahlian pelaksana pengelolaan keamanan informasi; (3) Instansi tidak mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata).

Area Pengelolaan Risiko Keamanan Informasi

Pada pengelolaan risiko keamanan informasi, nilai yang didapat sebesar 50 dari total 72 (69.44%). Dilihat dari jawaban dan kondisi yang terjadi, hasil penilaian area ini mengarah pada penerapan sebagian untuk pengelolaan risiko keamanan. Hal ini menunjukkan bahwa kebijakan terhadap risiko keamanan masih belum baik. Beberapa hal yang terkait dengan masalah risiko keamanan, seperti: kebijakan pengelolaan risiko keamanan informasi, dampak kerugian terkait dengan hilangnya fungsi aset utama, tindakan mitigasi dalam penanggulangan risiko yang terjadi masih sebagian diterapkan.

Area Kerangka Kerja Keamanan Informasi

Pada kerangka kerja keamanan informasi, nilai yang didapat sebesar 36 dari total 159 (22.64%). Dilihat dari jawaban dan kondisi yang terjadi, kerangka kerja keamanan informasi masih dalam perencanaan. Hal ini menunjukkan bahwa kesadaran akan penyusunan dan pengelolaan kerangka kerja keamanan informasi masih tidak baik. Beberapa hal terkait dengan kerangka kerja keamanan informasi yang masih dalam perencanaan, yaitu: pembuatan dokumen dan prosedur keamanan informasi, bagaimana konsekuensi dari pelanggaran kebijakan keamanan informasi, perencanaan pemulihan bencana terhadap layanan TIK, *monitoring* dan evaluasi terhadap kebijakan keamanan informasi yang dilakukan secara berkala, pelaksanaan audit internal termasuk evaluasi dan pelaporannya kepada pimpinan instansi terkait keamanan informasi, serta bagaimana rencana dan program peningkatan keamanan informasi untuk jangka pendek/menengah/panjang (1-3-5 tahun) yang direalisakan secara konsisten.

Area Pengelolaan Aset Informasi

Pada pengelolaan aset informasi, nilai yang didapat sebesar 88 dari total 168 (52.38%). Dilihat dari jawaban dan kondisi yang ada, pengelolaan aset informasi masih dalam perencanaan dan ada sebagian dilakukan. Hal ini menunjukkan bahwa pengelolaan inventarisasi terhadap aset informasi dan aset yang berhubungan dengan proses teknologi informasi, tata tertib penggunaan komputer, email, dan internet, pengelolaan identitas elektronik, prosedur *backup* dan *restore* data pada seluruh sistem elektronik, pelaporan insiden keamanan informasi kepada pihak eksternal (pihak yang berwajib), pengamanan terkait peraturan untuk mengamankan lokasi kerja penting (ruang *server*, ruang arsip) dari risiko yang membahayakan seperti larangan penggunaan handphone dan kamera di dalam ruang *server* masih belum baik.

Area Teknologi dan Keamanan Informasi

Pada teknologi dan keamanan informasi, nilai yang didapat sebesar 81 dari total 120 (67.5%). Dilihat dari jawaban dan kondisi yang ada, teknologi dan keamanan informasi masih sebagian dilakukan. Pengamanan teknologi masih belum dilakukan dengan baik. Kondisi ini meliputi konfigurasi standar untuk setiap komputer dan secara rutin dievaluasi, bagaimana pencatatan aktivitas pengguna di *log file*, bagaimana pengelolaan dan penerapan pergantian *password* secara rutin, dan menon-aktifkan *password* yang sudah tidak digunakan, pengamanan terhadap aset jaringan dan sistem elektronik, bagaimana pelaporan penyerangan *virus/malware* yang ditindaklanjuti dan diselesaikan.

Rekomendasi

Pada bagian ini akan diberikan rekomendasi (saran perbaikan) yang berdasarkan pada ISO/IEC 27002:2013. Berikut ini rekomendasi yang dapat dipertimbangkan untuk memperbaiki penilaian pengamanan informasi yang masih kurang, sebagai berikut:

- Perlu membuat kebijakan pengamanan informasi yang kompleks, seperti: kebijakan kontrol akses, pengklasifikasian informasi, keamanan fisik dan lingkungan terkait TIK, *backup* dan *restore* data, kebijakan dalam mentransfer informasi ke pihak eksternal, kebijakan pengamanan terhadap pembatasan pemasangan *software* di setiap komputer.
- Melakukan *review*, evaluasi, dan pelaporan terhadap kebijakan pengamanan informasi yang telah diterapkan tersebut.
- Pengaturan yang lengkap dan tegas terkait tanggungjawab dan peran personil terhadap keamanan informasi. Perlunya pemisahan tanggungjawab/tugas personil yang terkait langsung dengan pengoperasian TI. Pelaporan terkait *monitoring* perangkat TI dan kinerja dari personil tersebut. Hal ini dapat digunakan untuk mengevaluasi risiko yang disebabkan dari personil.
- Melakukan inventarisasi terhadap seluruh aset TI, termasuk aset informasi, perangkat lunak, detail dari *software* yang digunakan pada seluruh komputer, pemilik dari aset elektronik seperti laptop (detail personil yang bersangkutan, proses pengembalian aset setelah tidak lagi menggunakannya).
- Perlu ada kebijakan pengelolaan akses pengguna yang baik. Siapa saja pengguna yang teregistrasi di seluruh sistem, siapa saja pengguna yang sudah tidak aktif lagi, pengelolaan terhadap hak akses pengguna (hak akses ke sistem elektronik disesuaikan dengan tugas dari pengguna).

KESIMPULAN

Dari hasil evaluasi internal yang dilakukan terkait pengamanan informasi menggunakan indeks KAMI, maka kondisi kesiapan (kelengkapan dan kematangan) pengamanan informasi pada Diskominfo Kota Palembang, yaitu: penilaian kelengkapan program kerja pengamanan informasi sebesar 338. Sesuai dengan ketentuan indeks KAMI, maka hal ini berarti status kesiapan Diskominfo Kota Palembang masih perlu perbaikan. Sedangkan untuk penilaian tingkat kematangan pengamanan informasi pada Diskominfo Kota Palembang berada pada tingkat I-II. Hal ini berarti tingkat kematangan pengamanan informasi masih dalam kondisi awal dan sedang menerapkan kerangka kerja pengamanan informasi di dalam aktivitas penggunaan teknologi informasi.

DAFTAR KEPUSTAKAAN

Firmana, R., Hidayanto, B. C., & Astuti, H. M. (2013). Penggunaan Indeks Keamanan Informasi (KAMI) Sebagai Evaluasi Keamanan Informasi Pada PT. PLN Distribusi Jatim. *Jurnal Teknik POMITS*, *1*(1), 1–5.

Gunawan, C. E. (2020). Penerapan Metode TOPSIS untuk Pengangkatan Karyawan Kontrak Menjadi Karyawan Tetap (Studi Kasus: PT Hanuraba Sawit Kencana). *JIKO (Jurnal Informatika dan Komputer)*, *3*(1), 42–50. https://doi.org/10.33387/jiko.v3i1.1722

Gunawan, C. E., & Fenando, F. (2018). Pengukuran Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Studi Kasus di PUSTIPD UIN Raden Fatah Palembang. *JUSIFO (Jurnal Sistem Informasi)*, *4*(2), 121–132. https://doi.org/10.19109/JUSIFO.V4I2.4107

Gunawan, C. E., Ramadhan, M., & Indrawan, I. (2013). Sistem Informasi Seleksi Calon Mahasiswa Berbasis Web Di Sekolah Tinggi Teknik Musi Palembang. *Juita*, *II*(4). https://doi.org/10.30595/JUITA.V2I4.823

ISO Members. (2013). *International Standar ISO/IEC 27002:2013, Security techniques, Code of practice for information security controls*. International Organization for Standardization.

Putra, E. A. (2015). Anak berkesulitan Belajar di Sekolah Dasar Se-kelurahan Kalumbuk Padang. *E-JUPEKHU (Jurnal Ilmiah Pendidikan Khusus)*, *4*(3), 71–76.

Putra, E. L., Hidayanto, B. C., & Astuti, H. M. (2014). Evaluasi Keamanan Informasi Pada Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk. Dengan Menggunakan Indeks Keamanan Informasi (KAMI). *Jurnal Teknik POMITS*, *2*(1), 1–6.

Rahardjo, B. (2017). *Keamanan Informasi*. PT. Insan Infonesia. http://budi.rahardjo.id/files/keamanan.pdf

Ridho, M. R., Ghozali, K., & Hidayanto, B. C. (2012). Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan SNI ISO/IEC 27001:2009 Studi Kasus: Bidang Aplikasi dan Telematika Dinas Komunikasi Dan Informatika Surabaya. *JURNAL TEKNIK POMITS (Publikasi Online ITS)*, *1*(1), 1–6.

Saputra, D., & Gilang, O. (2016). Evaluasi Keamanan Informasi pada SMA Islam Al-Azhar (SMAIA) 4 Kemang Pratama Berdasarkan Indeks Keamanan Informasi (KAMI) SNI ISO/IEC 27001:2009. In *Jurnal Khatulistiwa Informatika* (Vol. 4, Nomor 1). https://doi.org/10.31294/JKI.V4I1.1254

Setiawan, A. B. (2013). Kajian Kesiapan Keamanan Informasi Instansi Pemerintah Dalam Penerapan E-Government. *Jurnal Masyarakat Telematika dan Informasi*, *4*(2), 109–126.

Tim Direktorat Keamanan Informasi. (2011). *Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik* (2.0). Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika RI.

Tim Penyusun Indeks KAMI 3.1. (2015). *Panduan Indeks Keamanan Informasi (KAMI) Versi 3.1*.