EVALUASI KEAMANAN SISTEM INFORMASI PASDEAL BERDASARKAN INDEKS KEAMANAN INFORMASI (KAMI) ISO/IEC 27001:2013

Yahya Dwi Wijaya
Universitas PGRI Madiun
Madiun, Indonesia
yahyadwi51@gmail.com

ABSTRACT

Information systems are a valuable asset for business actors, one of which is engaged in e-commerce. Pasdeal is a credit distributor and server service that implements an e-commerce information system. The use of information systems in the field of sales or electronic commerce is considered efficient because it has become a platform for media and services and new and unique capabilities that are not found in the physical world. Information security factor is a very important aspect to consider considering the performance of ICT governance. For this reason, information systems need an information security evaluation in order to find out the gaps and deficiencies in information security in the information system. The KAMI index is a reference tool to evaluate the level of readiness of information system security in an organization. Evaluation is carried out on various areas that are the target of information security implementation based on the ISO/IEC 27001:2013 standard. Based on the results of the KAMI index assessment, it was found that Pasdeal got a score of 591 points from the application of the ISO 27001 standard with a pretty good predicate.

Keyword: *ISO 27001:2013, KAMI Index, System Security.*

PENDAHULUAN

Saat ini seiring dengan perkembangan zaman, rasanya teknologi informasi menjadi hal yang selalu melekat dalam kehidupan sehari hari (Setiawan dkk., 2017). Teknologi dibutuhkan setiap orang saat melakukan berbagai macam pekerjaan. Tujuan pemanfaatan teknologi adalah untuk membantu dan mempermudah dalam melakukan pekerjaan (Purnama & SE, 2016). Dengan adanya sistem informasi merupakan salah satu hasil penerapan kemajuan teknologi informasi. Komponen yang membentuk adanya sistem informasi adalah perangkat keras (*hardware*), perangkat

lunak *(software*), data, orang-orang (*people*), serta jaringan komunikasi (*networks*) (Akil, 2018) . Adanya sistem informasi dapat memberikan kemudahan bagi pelaku usaha. Sistem informasi menjadi aset yang berharga bagi pelaku usaha, salah satunya adalah yang bergerak pada bidang dibidang penjualan. Penggunaan sistem informasi atau perdagangan elektronik dinilai efisien karena, dapat menjadi media dan layanan yang memiliki keunikan bukan berbentuk fisik melainkan dengan bentuk digital (Romindo dkk., 2019).

Namun, dibalik segala kemudahan dan peluang yang didapatkan, harus ada keseriusan dalam pengelolaan teknologi. Ada faktor yang harus diperhatikan dalam pengelolaan teknologi informasi agar tidak menimbulkan hal - hal yang tidak diinginkan (Manuhutu dkk., 2021). Salah satu faktor yang menjadi perhatian dan memiliki risiko adalah faktor keamanan informasi. Hal ini dikarenakan teknologi informasi dan komunikasi bisa saja mengalami gangguan atau bermasalah jika informasi sebagai salah satu objek utamanya mengalami masalah terhadap keamanan informasi (Sari dkk., 2020). Keamanan informasi ini menyangkut kerahasiaan, keutuhan dan ketersediaan. Dalam rangka pengamanan informasi, sistem informasi perlu adanya evaluasi keamanan informasi agar mengetahui celah dan kekurangan dibagian keamanan informasi (Siswanti, 2021). Langkah - langkah evaluasi harus sesuai kerangka yang memiliki standart nasional maupun internasional. Dalam penelitian ini, penulis melakukan evaluasi keamanan informasi berdasarkan indexs keamanan informasi (KAMI) berdasarkan ISO/IEC 7001:2013 pada sistem informasi Pasdeal. Indeks KAMI yang digunakan dalam penelitian ini merupakan versi keluaran terbaru yaitu versi 4.1 yang diterbitkan oleh Badan Siber Sandi Negara (BSSN) (Riswaya dkk., 2020).

Pasdeal adalah bentuk layanan *e-commerce* yang bergerak dibidang distributor & server pulsa. Pasdeal mulai diluncurkan sejak tahun 2018 dengan jumlah pelanggan yang mengakses sistem sekitar 1000 pelanggan. Sejak diluncurkan pada tahun 2018 silam, sistem informasi pasdeal belum pernah dilakukan evaluasi berdasarkan standart ISO khususnya pada bidang keamanan informasi. Keterikatan terhadap teknologi

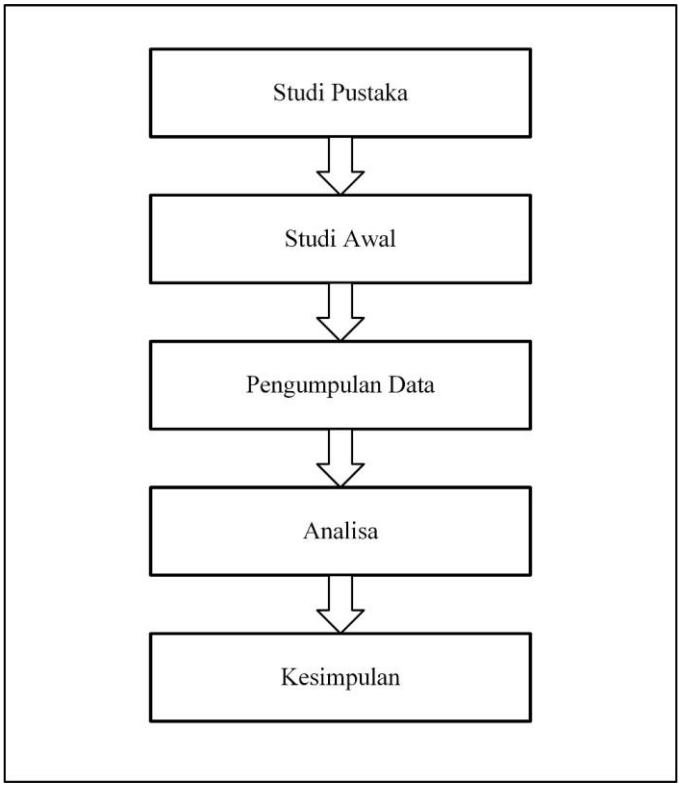
bukan hanya memberikan dampak positif saja, melainkan ada kemungkinan dampak negatif yang ditimbulkan akibat minimnya pengetahuan akan keamanan informasi (Triandi, 2019). Sistem informasi pasdeal tentu mebutuhkan analisa guna mengetahui seberapa besar kesiapan mempersiapkan keamanan informasi sesuai standart yang berlaku.

Analisia tingkat kelengkapan dan tingkat kematangan keamanan informasi pada sistem informasi Pasdeal menggunakan indeks Keamanan Informasi (KAMI). Sektor yang menjadi fokus analisa terdiri dari aspek pengelolaan risiko, keamanan informasi, teknologi, kerangka kerja keamanan informasi, pengelolaan aset informasi, tata kelola keamanan informasi dan keamanan informasi (Yunella dkk., 2020). Penggunaan indeks KAMI merupakan langkah kerja evaluasi yang digunakan untuk analisa tingkat keamanan informasi di suatu organisasi (Husin dkk., 2017). Tolak ukur evaluasi ini tidak ditujukan untuk menganalisa kelayakan bentuk pengamanan yang ada, tetapi sebagai tolak ukur untuk memberikan gambaran kondisi kesiapan kerangka kerja keamanan informasi kepada pimpinan organisasi (Azis, 2017).

Pada penelitian ini akan dilakukan analisa terkait keamanan teknlogi informasi yang ada pada Pasdeal, dimana metode yang digunakan berdasrakan kerangka kerja Indeks Keamanan Informasi (KAMI). Kerangka kerja indeks KAMI terdapat beberapa bagian diantaranya adalah evaluasi sistem elektronik, tata kelola, resiko, kerangka kerja, pengelolaan aset, teknologi, dan suplemen. 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 27001:2013 (Musyarofah & Bisma, 2021). Sehingga dapat memberikan hasil analisa berupa temuan masalah dan rekomendasi kemanan informasi di sistem infrormasi Pasdeal dan sekaligus menjadi tujuan penelitian ini. Adanya hasil analisa diharapkan mampu mejadi dasar acuan pengembangan sistem informasi.

METODE

Pada tahap metode kali ini dibahas mengenai metode, tahapan, maupun model yang digunakan dalam penelitian yang dilakukan. Tahapan penelitian dalam melakukan evaluasi keamanan sistem dan teknologi informasi dengan menggunakan indeks keamanan informasi berdasarkan ISO/IEC 27001:2013(Ferdiansyah dkk., 2019). Berikut tahapan penelitian yang dilakukan.



Gambar 1. Alur Penelitian

1. Studi Pustaka

Tahap pertama dalam penelitian ini adalah melakukan studi pustaka dengan mencari informasi mengenai indeks KAMI 4.1 dan mencari topik penelitian yang akan dijadikan bahan acuan dalam penelitian ini. Pencarian pustaka yang diperoleh berasal dari buku dan jurnal.

2. Studi Awal

Tahap kedua adalah studi awal yaitu dengan mempelajari dan melihat langsung lingkungan yang menjadi objek penelitian.

3. Pengumpulan Data

Pengumpulan data yang dilakukan menggunakan teknik wawancara yang dilakukan kepada pemilik sistem informasi Pasdeal dan staff IT yang bertujuan untuk menggali informasi lebih dalam terkait sistem informasi Pasdeal. Pada tahapan ini mulai melakukan wawancara dan mengisi *kuesioner* berdasarkan kerangka kerja Indeks Keamanan Informasi (KAMI). Menggunakan *kuesioner* untuk mengumpulkan data yang dilakukan dengan mengadakan komunikasi dengan sumber data.

3.1 Bagian Sistem Elektronik

Bagian ini dilakukan analisa sistem elektronik karena untuk mengetahui tingkat ketergantungan proses bisnis terhadap teknologi informasi.

1.6	Data pribadi yang dikelola Sistem Elektronik [A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya [B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha [C] Tidak ada data pribadi	A
1.7	Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Sangat Rahasia [B] Rahasia dan/atau Terbatas [C] Biasa	B
1.8	Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik [B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung [C] Proses yang hanya berdampak pada bisnis perusahaan	C
1.9	Dampak dari kegagalan Sistem Elektronik [A] Tidak tersedianya layanan publik berskala nasional atau membahayakan pertahanan keamanan negara [B] Tidak tersedianya layanan publik dalam 1 propinsi atau lebih [C] Tidak tersedianya layanan publik dalam 1 kabupaten/kota atau lebih	C
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme) [A] Menimbulkan korban jiwa [B] Terbatas pada kerugian finansial [C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan mengakibatkan kerugian finansial)	C
	Skor penetapan Kategori Sistem Elektronik	**18**

Gambar 2. Tingkatan Nilai Kategori SE Indeks KAMI

3.2 Bagian Tata Kelola Keamanan Informasi.

Organisasi harus mampu mempersiapkan bentuk tata kelola keamanan informasi yang terbagi dalam masing masing tugas yang diberikan kepada pengelola atau staff IT. Pada bagian ini memberi acuan tentang tingkat tanggung jawab pengelola keamanan sistem.

2.13	II	2	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?	Diterapkan Secara Menyeluruh
2.14	III	2	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?	Diterapkan Secara Menyeluruh
2.15	III	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan instansi/perusahaan secara rutin dan resmi?	alam Penerapan / Diterapkan Sebagia
2.16	III	2	Apakah kondisi dan permasalahan keamanan informasi di instansi/perusahaan anda menjadi konsiderans atau bagian dari proses pengambilan keputusan strategis di instansi/perusahaan anda?	Diterapkan Secara Menyeluruh
2.17	IV	3	Apakah pimpinan satuan kerja di instansi/perusahaan anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	Diterapkan Secara Menyeluruh
2.18	IV	3	Apakah instansi/perusahaan anda sudah mendefinisikan metrik, parameter dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?	alam Penerapan / Diterapkan Sebagia
2.19	IV	3	Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Diterapkan Secara Menyeluruh
2.20	IV	3	Apakah instansi/perusahaan anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan instansi/perusahaan?	Diterapkan Secara Menyeluruh
2.21	IV	3	Apakah instansi/perusahaan anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	Diterapkan Secara Menyeluruh
2.22	IV	3	Apakah instansi/perusahaan anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Diterapkan Secara Menyeluruh
			Total Nilai Evaluasi Tata Kelola	**116**

Gambar 4. Indeks KAMI Bagian Tata Kelola Keamanan Sistem Informasi.

3.3 Bagian Resiko Kemanan Informasi

Risiko kemanan informasi tidak bisa dihindari, tetapi bisa diminimalisir. Unutk itu dalam bagian risiko keamanan mendefinisikan langkah untukgevaluasi kesiapan pengolahan risiko kemanan yang harus diterapkan agar sistem bisa meminimalisir risiko.

3.7	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	alam Penerapan / Diterapkan Sebagia
3.8	II	1	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	Diterapkan Secara Menyeluruh
3.9	II	1	Apakah instansi/perusahaan anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?	alam Penerapan / Diterapkan Sebagia
3.10	II	1	Apakah instansi/perusahaan anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	alam Penerapan / Diterapkan Sebagia
3.11	III	2	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?	Diterapkan Secara Menyeluruh
3.12	III	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	Diterapkan Secara Menyeluruh
3.13	IV	2	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?	Diterapkan Secara Menyeluruh
3.14	IV	2	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?	Diterapkan Secara Menyeluruh
3.15	V	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	Diterapkan Secara Menyeluruh
3.16	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	alam Penerapan / Diterapkan Sebagia
			Total Nilai Evaluasi Pengelolaan Risiko Keamanan Informasi	**65**

Gambar 3. Indeks KAMI Bagian Resiko Keamanan Informasi

3.4 Bagian Kerangka Kerja Pengolahan Keamanan Informasi

Bagian yang menjadi pusat perhatian kesiapan kerja berisi tentang kerangka kerja, kebijakan & prosedur. Aspek tersebut digunakan untuk salah satu langkah langkah penerapan keamanan informasi.

4.20	II	1	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	Diterapkan Secara Menyeluruh
4.21	II	1	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?	Diterapkan Secara Menyeluruh
4.22	III	1	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	Diterapkan Secara Menyeluruh
4.23	III	1	Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?	alam Penerapan / Diterapkan Sebagia
4.24	III	1	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi?	Diterapkan Secara Menyeluruh
4.25	III	2	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	Diterapkan Secara Menyeluruh
4.26	III	2	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	Diterapkan Secara Menyeluruh
4.27	IV	3	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?	Diterapkan Secara Menyeluruh
4.28	V	3	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pembenahan yang diperlukan, telah diterapkan secara efektif?	alam Penerapan / Diterapkan Sebagia
4.29	V	3	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	Diterapkan Secara Menyeluruh
			Total Nilai Evaluasi Kerangka Kerja	**143**

Gambar 6. Indeks KAMI Bagian Kerangka Kerja Pengolahan Keamanan

3.5 Bagian Pengelolaan Aset

Bagian ini mengevaluasi tentang kelengkapan pengamanan aset informasi. Didalam bagian pengelolaan aset juga mendefinisikan keseluruhan siklus penggunaan aset yang dilakukan oleh organisasi.

5.30	II	1	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?	alam Penerapan / Diterapkan Sebagia
5.31	II	1	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	Diterapkan Secara Menyeluruh
5.32	II	1	Apakah tersedia peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor)?	alam Penerapan / Diterapkan Sebagia
5.33	II	1	Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris)?	Diterapkan Secara Menyeluruh
5.34	II	2	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?	Diterapkan Secara Menyeluruh
5.35	II	2	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	Diterapkan Secara Menyeluruh
5.36	II	2	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	Diterapkan Secara Menyeluruh
5.37	II	2	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)	Diterapkan Secara Menyeluruh
5.38	III	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan anda?	Diterapkan Secara Menyeluruh
			Total Nilai Evaluasi Pengelolaan Aset	**155**

Gambar 7. Indeks KAMI Bagian Pengelolaan Aset

3.6 Bagian Teknologi

Pada bagian ini, peran teknologi bisa dilihat pada aspek kelengkapan, konsistensi serta tingkat efektif dalam penggunaan teknologi. Tingkatan akan mempengaruhi kelayakan tingkat pengamanan informasi pada sistem informasi Pasdeal.

6.15	III	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	Diterapkan Secara Menyeluruh
6.16	III	2	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts* , *lockout* setelah kegagalan *login* ,dan penarikan akses?	Diterapkan Secara Menyeluruh
6.17	III	2	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	Diterapkan Secara Menyeluruh
6.18	II	1	Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?	Diterapkan Secara Menyeluruh
6.19	II	1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	Diterapkan Secara Menyeluruh
6.20	II	1	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	Diterapkan Secara Menyeluruh
6.21	III	2	Apakah ada rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	alam Penerapan / Diterapkan Sebagia
6.22	III	2	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	alam Penerapan / Diterapkan Sebagia
6.23	III	2	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Diterapkan Secara Menyeluruh
6.24	III	2	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?	Diterapkan Secara Menyeluruh
6.25	III	3	Apakah instansi/perusahaan ada menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?	Diterapkan Secara Menyeluruh
6.26	IV	3	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Diterapkan Secara Menyeluruh
			Total Nilai Evaluasi Teknologi dan Keamanan Informasi	**112**

Gambar 8. Indeks KAMI Bagian Teknologi

3.7 Bagian Suplemen

Pada bagian mengevaluasi kelengkapan, konsistensi serta tingkat efektif dalam penggunaan teknologi dalam pengamanan aset informasi.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
7.1			**Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan**		2,81
7.1.1			**Manajemen Risiko dan Pengelolaan Keamanan pihak ketiga**		
7.1.1.1		1	Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?	Diterapkan Secara Menyeluruh	3
7.1.1.2		1	Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?	Diterapkan Secara Menyeluruh	3
7.1.1.3		1	Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?	Diterapkan Secara Menyeluruh	3
7.1.1.4		1	Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?	Diterapkan Secara Menyeluruh	3
7.1.1.5		1	Apakah instansi/perusahaan telah menerapkan kebijakan keamanan informasi bagi pihak ketiga secara memadai, mencakup persyaratan pengendalian akses, penghancuran informasi, manajemen risiko penyediaan layanan pihak ketiga, dan NDA bagi karyawan pihak ketiga?	Diterapkan Secara Menyeluruh	3
7.1.1.6		1	Apakah kebijakan tersebut (7.1.1.5) telah dikomunikasikan kepada pihak ketiga dan mereka menyatakan persetujuannya dalam dokumen kontrak, SLA atau dokumen sejenis lainnya?	Diterapkan Secara Menyeluruh	3
7.1.1.7		1	Apakah hak audit TI secara berkala ke pihak ketiga telah ditetapkan sebagai bagian dan persyaratan kontrak, dikomunikasikan dan disetujui pihak ketiga? Termasuk di dalamnya akses terhadap laporan audit internal/eksternal tentang kondisi kontrol keamanan informasi pihak ketiga?	Diterapkan Secara Menyeluruh	3
7.1.2			**Pengelolaan Sub-Kontraktor/Alih Daya pada Pihak Ketiga**		
7.1.2.1		1	Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan dalam layanannya?	alam Penerapan / Diterapkan Sebagia	2
7.1.2.2		1	Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?	Diterapkan Secara Menyeluruh	3
7.1.2.3		1	Apakah pihak ketiga melakukan pemantauan dan evaluasi terhadap kepatuhan alih daya, subkontraktor atau penyedia teknologi/infrastruktur terhadap persyaratan keamanan yang ditetapkan?	alam Penerapan / Diterapkan Sebagia	2

Gambar 8. Indeks KAMI Bagian Supemen

4. Analisa

Setelah melakukan wawancara dan pengisian kuesioner indeks KAMI, data yang diolah dijadikan dasar sebagai acuan analisa temuan masalah dan rekomendasi perbaikan (Gala dkk., 2020).

5. Kesimpulan

Hasil evaluasi kemudian dianalisis untuk mendapatkan rumusan beberapa kesimpulan yang dapat diambil dari penelitian.

HASIL DAN PEMBAHASAN

1. Analisa Penilaian Bagian Sistem Elektronik

Bagian Sistem elektronik memliki nilai sebesar 18 yang berarti memiliki tingkat ketergantungan tinggi terhadap teknologi. Nilai yang tinggi salah satunya dipengaruhi adanya temuan bahwa organisasi menerapkan teknik kriptografi sesuai standart atau dikembangkan sendiri. Fungsi kriptografi adalah untuk menjaga isi data atau pesan sehingga orang lain yang tidak memiliki hak dan wewenang tidak bisa mengerti arti dari data tersebut.

Tabel 1. Tabel Kategori Sistem Elektronik

Kategori Sistem Elektronik	Nilai Skor
Rendah	10-15
Tinggi	16-34
Strategis	35-50

Memiliki nilai yang tinggi bukan berarti mempunya kekurangan, ada beberapa kekurangan yang harus ditingkatkan agar nilai indeks bagian sistem elektronik ini bisa bertambah. Rekomendasi perbaikan yang harus dilakukan adalah kepatuhan akan peraturan atau standart nasional maupun internasional. Rekomendasi perbaikan lainnya agar nilai indeks sistem elektronik dapat bertambah adalah dengan menargetkan pengguna sistem diatas 5000 orang yang semula hanya kisaran 1000 orang.

2. Analisa Penilaian Bagian Tata Kelola

Pada bagian tata kelola mempunya nilai sebesar 116 yang berarti masih berada ditingkat III. Faktor yang menonjol dibagian tata kelola keamanan informasi adalah ada di integrasi keamanan di proses kerja sistem informasi Pasdeal. Selain integrasi keamanan, standart kemampuan dan keahlian juga mempengaruhi nilai yang didapat pada tata kelola keamanan informasi. Berada pada tingkatan ke III masih perlu adanya perbaikan, rekomendasi perbaikan dengan menerapkan kebijakan yang dilakukan untuk menanggulangi insiden keamanan informasi yang menyangkut pelanggaran hukum.

3. Analisa Penilaian Bagian Resiko Keamanan Informasi

Memeroleh nilai sebesar 65 dan berada pada tingkatan IV, membuat bagian resiko sudah sangata baik. Namun bagian keamanan masih membutuhkan perbaikan diberbagai sektor dalam risiko keamanan. Kelebihan yang dimiliki pada sistem informasi Pasdeal ada pada identifikasi ancaman ases informasi. Sehingga pada bagian itu memiliki nilai yang tinggi. Ada bebarapa rekomendasi perbaikan pada aspek risiko keamanan informasi diantanya, perlu adanya identifikasi dampak kerugian terkait terganggunya aset. Rekomendasi perbaikan lainnya adalah adanya langkah mitigasi risiko secaraberkala. Tujuannya adalah unutk memastikan penyelesaian dan kemajuan kinerja.

4. Analisa Penilaian Bagian Kerangka Kerja Keamanan Informasi

Pasdeal mendapatkan nilai 143 dengan berada pada tingkat III pada bagian kerangka kerja. Salah satu penyumbang nilai banyak pada kerangka kerja keamanan informasi ada pada, keterbukaan kebijakan kemanan informasi kepada staff organisasi. Dalam pengembangan sistem infromasi, Pasdeal sudah melakukan teknik pengembangan sesuai standart metode. Namun ada beberapa rekomendasi yang diberikan untuk perbaikan dalam bidang kerangka kerja adalah perlu adanya audit internal untuk kepatuhan maupun konsistensi dalam pengelolaan keamanan

informasi. Selain melakukan audit internal, penting juga untuk melakukann uji evaluasi secara berkala terkait pengelolaan keamanan informasi.

5. Analisa Penilaian Bagian Pengelolaan Aset

Memiliki nilai sebesar 155 membuat bagian pengelolaan aset Pasdeal berada ditingkat III. Pengelolaan aset Pasdeal masih memerlukan perbaikan juga. Namun sebagian sudah diterapkan secara menyeluruh seperti, adanya tata tertib atau aturan penggunaan email maupun komputer organisasi. Tak hanya tata tertib, factor lain penyumbang nilai adalah karena memiliki kebijakan prosedur tentang data back – up dan penghapusan aset aset yang tidak penting. Ada temuan rekomendasi pada bagian pengelolaan aset diantaranya, menerapkan proses pengelolaan perubahan terhadap sistem maupun proses bisnis. Pasdeal dalam pengelolaan aset belum menerapkan proses pengelolaan perubahan secara konsisten.

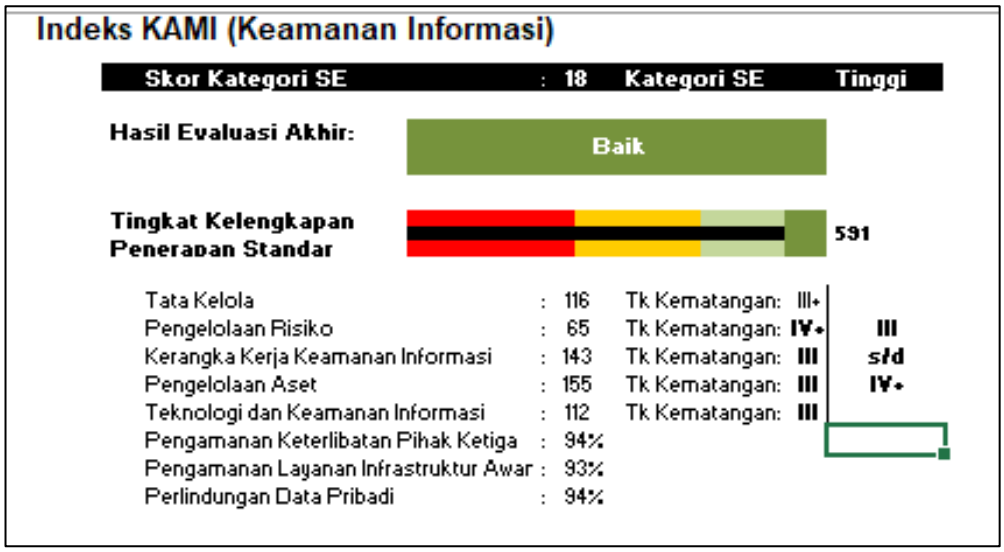
6. Analisa Penilaian Bagian Teknologi dan Keamanan Sistem Informasi

Pasdeal memiliki nilai sebesar 112 dibagian teknologi keamanan sistem informasi sehingga berada ditingkat III. Penerapan jaringan komunikasi sesuai kepentingan menjadi faktor penyumbang nilai di bagian teknolologi. Adanya monitoring jaringan membuat keamanan sistem informasi Pasdeal bisa dikatakan baik. Berada ditingkat II membuat bagian teknologi dan keamanan perlu adanya perbaikan. Rekomendasi yang diberikan untuk memperbaiki tingkatan teknologi dan keamanan diantaranya, penerapan antivirus di server maupun desktop. Malware dapat memberi dampak buruk karena penyerangan dapat mencuri informasi ataupun data pribadi. Temuan rekomendasi perbaikan juga mengacu pada kajian kehandalan keamanan sistem secara rutin yang belum diterapkan di Pasdeal.

7. Analisa Penilaian Bagian Suplemen

Hasil evaluasi pada tahapan suplemen diperoleh tingkat kematangan untuk pengamanan keterlebitan pihak ketiga sebesar 94%. Kemudian untuk pengamanan layanan infrastruktur awan sebesar 93% dan yang terakhir yaitu perlindungan data pribadi sebesar 94%.

Berdasarkan pengukuran dari wawancara berdasarkan kuesioner indeks KAMI pada sistem informasi Pasdeal membuahkan hasil data berupa diagram batang. Kuesioner berdasarkan pada 7 bagian evaluasi yang disesuaikan dengan kerangka kerja Indeks KAMI. Bagian tersebut adalah evaluasi sistem elektronik, tata kelola, resiko, kerangka kerja, pengelolaan aset, teknologi, dan suplemen. Hasil data akan menjadi bahan acuan evaluasi dan perbaikan pada sistem informasi Pasdeal.



Gambar 9. Bagan Hasil Indeks KAMI

Terdapat keterangan hasil evaluasi akhir menunjukkan nilai 591, sistem informasi Pasdeal sudah menerapkan sebagaian besar dari tata kelola sistem informasi yang baik dan sesuai dengan kebutuhan. Namun masih ditemukan juga kelemahan-kelemahan yang ada di beberapa bagian terkait keamanan dari data dan informasi yang

ada. Nilai sebesar 591 memiliki status evaluasi akhir dikatakan Baik berdasarkan acuan pada range penilaian berikut ini (Purwanto & Huda, 2019).

Tabel. Range Skor Indeks KAMI

Skor Akhir	Status Kesiapan
0-174	Tidak Layak
175-312	Perlu Perbaikan
313-535	Cukup
536-645	Baik

Selain hasil dari tingkat kelengkapan standart ISO27001 di dalam evaluasi tersebut didapati bahwa sudah mulai ada rasa ketergantungan dan menganggap TIK itu penting, sehingga nilai dari tingkat ketergantungan dari Pasdeal terhadap TIK juga tinggi. Tinkgat ketergantungan tersebut dibuktikan pada nilai kategori sistem elektronik dengan jumlah 18 yang berarti kategori tinggi. Hal ini mendasari bahwa kebutuhan akan TIK semakin banyak dan semakin hari terus berkembang.

Sistem Informasi Pasdeal masih memerlukan perbaikan diberbagai sektor agar nilai tingkat kelengkapan penerapan standart ISO bisa lebih tinggi. Perbaikan dilakukan agar Pasdeal dapat mempersiapkan diri untuk sertifikasi ISO 27001 dengan tingkat kematangan lebih dari tingkat III.

KESIMPULAN

Penelitian yang dilakukan pada sistem informasi Pasdeal, telah dilakukan dan hasil dari penelitian memaparkan bahwa sistem informasi Pasdeal mendapatkan tingkat penerapan standart ISO 27001 dengan predikat Baik. Total nilai yang diperoleh adalah 591 dari aspek penilaian berdasarkan analisa dan kuesioner menggunakan indeks KAMI. Dari nilai yang yang didapat sistem informasi Pasdeal berada di tingkat III yang artinya masih memerlukan sejumlah perbaikan.

DAFTAR PUSTAKA

Akil, M. A. (2018). Penerapan Sistem Informasi E-Business Di Indonesia: Prospek Dan Tantangan. *Jurnal Dakwah Tabligh*, *16*(2), 111–122.

Azis, M. S. (2017). Audit Keamanan Informasi Pada Pdam Tirta Tarum Karawang Menggunakan Indeks Kami Sni Iso/Iec 27001: 2009 Dan Fishbone. *Jurnal Inovasi Informatika*, *2*(2), 41–57.

Ferdiansyah, P., Subektiningsih, S., & Indrayani, R. (2019). Evaluasi Tingkat Kesiapan Keamanan Informasi Pada Lembaga Pendidikan Menggunakan Indeks Kami 4.0. *Mobile and Forensics*, *1*(2), 53–62.

Gala, R. A., Sengkey, R., & Punusingon, C. (2020). Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI. *Jurnal Teknik Informatika*, *15*(3), 189–198.

Husin, M. F., Wowor, H. F., & Karouw, S. (2017). Implementasi Indeks KAMI di Universitas Sam Ratulangi. *Jurnal Teknik Informatika*, *12*(1).

Manuhutu, M. A., Muttaqin, M., Irmayani, D., Tamara, T., Gustiana, Z., Hazriani, H., Manullang, S. O., Jamaludin, J., Iskandar, A., & Negara, E. S. (2021). *Pengantar Forensik Teknologi Informasi*. Yayasan Kita Menulis.

Musyarofah, S. R., & Bisma, R. (2021). Analisis kesenjangan sistem manajemen keamanan informasi (SMKI) sebagai persiapan sertifikasi ISO/IEC 27001: 2013 pada institusi pemerintah. *Teknologi: Jurnal Ilmiah Sistem Informasi*, *11*(1), 1–15.

Purnama, C., & SE, M. (2016). Sistem Informasi Manajemen. *Mojokerto: Penerbit Insan Global. Tersedia secara online juga di: http://dosen. stie-alanwar. ac. id/file/content/2018/04/chamdan_Purnama_sistem_informasi_manajemen [diakses di Surabaya, Jawa Timur, Indonesia: 15 Januari 2018]*.

Purwanto, F. H., & Huda, M. (2019). Pengukuran Tingkat Keamanan Informasi Perguruan Tinggi XYZ Menggunakan Indeks Keamanan Informasi (KAMI) Berbasis ISO/IEC-27001: 2013. *Jurnal VOI (Voice Of Informatics)*, *8*(2).

Riswaya, A. R., Sasongko, A., & Maulana, A. (2020). Evaluasi Tata Kelola Keamanan Teknologi Informasi Menggunakan Indeks Kami Untuk Persiapan Standar Sni Iso/Iec 27001 (Studi Kasus: Stmik Mardira Indonesia). *Jurnal Computech & Bisnis*, *14*(1), 10–18.

Romindo, R., Muttaqin, M., Saputra, D. H., Purba, D. W., Iswahyudi, M., Banjarnahor, A. R., Kusuma, A. H. P., Effendy, F., Sulaiman, O. K., & Simarmata, J. (2019). *E-Commerce: Implementasi, Strategi dan Inovasinya*. Yayasan Kita Menulis.

Sari, I. Y., Muttaqin, M., Jamaludin, J., Simarmata, J., Rahman, M. A., Iskandar, A., Pakpahan, A. F., Abdul Karim, S., Giap, Y. C., & Hazriani, H. (2020). *Keamanan Data dan Informasi*. Yayasan Kita Menulis.

Setiawan, D., Asnawi, N., & Mumtahana, H. A. (2017). Evaluation of style-teaching Lecturers Informatics Engineering Study Program UNIPMA in Trend Education Based on Technology. *Int. Conf. Educ. Sci*, 1168–1173.

Siswanti, S. (2021). Penilaian Kematangan Proses Keamanan Sistem Informasi Pendaftaran Pasien Menggunakan Framework Cobit 4.1. *SATIN-Sains dan Teknologi Informasi*, *7*(1), 123–133.

Triandi, B. (2019). Keamanan Informasi secara Aksiologi Dalam Menghadapi Era Revolusi Industri 4.0. *JURIKOM (Jurnal Riset Komputer)*, *6*(5), 477–483.

Yunella, M., Herlambang, A. D., & Putra, W. H. N. (2020). Evaluasi Tata Kelola Keamanan Informasi pada Dinas Komunikasi dan Informatika Kota Malang Menggunakan Indeks Kami. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN*, *2548*, 964X.