CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 7, No. 1, Mei 2024,, hlm. 7-17

Evaluasi Keamanan Sistem Informasi Pada Penyedia Layanan Cloud Dan Perlindungan Data Pribadi Berdasarkan Index Kami Versi 4.2 (Studi Kasus : PTIPD UIN Sunan Kalijaga Yogyakarta)

Faiz Akhmad Hafizuddin[1], Bambang Sugiantoro[2]
[1,2]Informatika Universitas Islam Negri Sunan Kalijaga Yogyakarta
Email: [1]23106050075@student.uin-suka.ac.id, [2]bambang.sugiantoro@uin-suka.ac.id

Abstrak

Pusat Teknologi Informasi Dan Pangkalan Data (PTIPD) merupakan salah satu Unit Pelaksana Teknis (UPT) yang ada di Universitas Islam Negri Sunan Kalijaga Yogyakarta yang memiliki tugas untuk mengelola dan mengembangkan sistem informasi manajemen, pengembangan, pemeliharaan jaringan dan aplikasi, pengelolaan basis data, pengembangan teknologi lainnya, dan kerjasama jaringan. Perkembangan teknologi yang pesat dan pola bisnis yang dinamis menyebabkan munculnya risiko keamanan informasi baru. Keterlibatan pihak ketiga penyedia layanan dalam suatu instansi menimbulkan risiko terkait keberadaan dan keterlibatan pihak eksternal. Layanan berbasis infrastruktur awan *(Cloud)* memberikan peluang efisiensi dan peningkatan kinerja yang sangat signifikan bagi instansi, akan tetapi risiko terkait data yang berada pada pengendalian pihak ketiga (penyelenggara layanan) perlu dimitgasi. Penggunaan *tools* indeks KAMI dalam penelitian ini hanya berfokus dalam tiga area diantaranya: pengamanan keterlibatan pihak ketiga, pengamanan layanan infrastrukutur awan dan perlindungan data pribadi. Hasil dari evaluasi tingkat presentase kelengkapan dan efektifitas penggunaan teknologi dalam pengamanan aset informasi di PTIPD UIN Sunan Kalijaga Yogyakarta yaitu: untuk pengamanan keterlibatan pihak ketiga mendapatkan presentase 49%, pengamanan layanan infrastruktur awan *(cloud)* sebesar 33% dan untuk pengamanan perlindungan data pribadi mendapatkan presentase 67%. Rekomendasi dari penelitian ini dapat di jadikan sebagai bahan pertimbangan da evaluasi bagi instansi dalam melakukan perbaikan yang berkaitan dengan mitigasi risiko dan pencegahan terhadap kerentanan keamanan informasi, serta dapat memastikan aturan dapat tercapai dengan baik dan keputusan terhadap kebijakan keamanan informasi dalam satu instansi di masa depan.

Kata kunci: Indeks KAMI, PTIPD, Keamanan Informasi, Penyedia Layanan Cloud, Perlindungan Data Pribadi

Evaluation Of Information System Security In Cloud Service Provider And Protection Of Personal Data Based On Index Kami Version 4.2 (Case Study: PTIPD UIN Sunan Kalijaga Yogyakarta)

Abstract

The Center for Information Technology and Database (PTIPD) is one of the Technical Implementation Units (UPT) at the Islamic University of Sunan Kalijaga, Yogyakarta, which has the task of managing and developing management information systems, developing, maintaining networks and applications, managing databases, developing other technologies, and network cooperation. Rapid technological developments and dynamic business patterns have led to the emergence of new information security risks. The involvement of third party service providers in an agency creates risks related to the presence and involvement of external parties. Cloud infrastructure-based services (Cloud) provide significant efficiency and performance improvement opportunities for agencies, but risks related to data that are in the control of third parties (service providers) need to be mitigated. The use of the KAMI index tools in this study focuses only on three areas including: securing third party involvement, securing cloud infrastructure services and protecting personal data. The results of evaluating the percentage level of completeness and effectiveness of using technology in securing information assets at PTIPD UIN Sunan Kalijaga Yogyakarta, namely: for securing third party involvement gets a percentage of 49%, securing cloud infrastructure services (cloud) for 33% and for securing personal data protection getting a percentage 67%. Recommendations from this research can be used as material for consideration and evaluation for agencies in making improvements related to risk mitigation and prevention of information security vulnerabilities, and can ensure that rules can be achieved properly and decisions on information security policies within an agency in the future.

Keywords: *KAMI Index, PTIPD, Information Security, Cloud Service Provider, Protection Of Personal Data*

1. PENDAHULUAN

Perkembangan teknologi yang pesat dan pola bisnis yang dinamis menyebabkan munculnya risiko keamanan informasi baru. Keterlibatan pihak ketiga dalam rantai pasok *(supply chain)* layanan suatu instansi atau perusahaan menimbulkan risiko terkait keberadaan dan keterlibatan pihak eksternal tersebut. Layanan berbasis infrastruktur awan *(Cloud)* memberikan peluang efisiensi dan peningkatan kinerja yang sangat signifikan bagi instansi atau perusahaan, akan tetapi risiko terkait data yang berada pada pengendalian pihak ketiga (penyelenggara layanan) perlu dimitgasi. Sedangkan disahkannya peraturan terkait perlindungan data pribadi oleh banyak negara memerlukan kerangka kerja yang secara spesifik membahas bagaimana data pribadi yang ada dan digunakan dalam instansi atau perusahaan diamankan sesuai dengan persyaratan hukum.

Teknologi informasi (TI) merupakan suatu yang penting bagi organisasi saat ini. Mulai dari membantu pekerjaan di level operasional sampai dengan membantu level strategis untuk mengambil keputusan. Hal tersebut mengakibatkan organisasi perlu untuk melakukan pengambilan keputusan terkait pengeluaran dana untuk membangun TI untuk memenuhi kebutuhannya.

Pada tahun 2017 institusi Pendidikan mendapat sorotan bagi dunia internasional karena mengalami peningkatan kebocoran data terbesar dibandingkan dengan sektor lain (Gemalto, 2017). Hal tersebut disebabkan jumlah data yang hilang meningkat secara signifikan, yaitu mencapai 32 juta data atau naik 4.957% (jika dibandingkan dengan semester lalu) di semester pertama tahun 2017. Ada satu kasus yang cukup fenomenal terkait kebocoran data pada tahun 2017 di institusi pendidikan. Persitiwa tersebut terjadi di Cina. Seorang mantan manager pemasaran di salah satu pendidikan swasta di Cina menjual jutaan informasi pribadi mahasiswa ke perusahaan. Hasil penjualan tersebut memberikan keuntungan pribadi oleh tersangka sebesar 10.000 Yuan atau US$1.450 (Huizhi, 2022).

Sehubungan dengan itu, organisasi yang terkena dampak kebocoran data harus menangani ataupun menyelesaikan kasus tersebut. Penanganan tersebut membutuhkan sejumlah biaya, seperti biaya untuk melakukan investigasi kasus kebocoran data. Menurut laporan dari Ponemon Institute LLC tahun 2017 (Ponemon Institute LLC, 2017) dinyatakan bahwa secara global biaya atas kejadian kebocoran data di institusi pendidikan, yaitu $200 per data yang hilang. Institusi pendidikan menduduki posisi ke-4 sebagai sektor dengan biaya tertinggi dalam penanganan kasus kebocoran data. Hal tersebut akan berdampak pada keuangan organisasi bahkan dapat berdampak kepada kepercayaan konsumen. Oleh sebab itu, para pelaku institusi pendidikan di seluruh dunia perlu melakukan tindakan preventif untuk mencegah kejadian kasus serupa termasuk Indonesia.

Indonesia juga mengalami kasus terkait keamanan informasi. Berdasarkan laporan dari ID-CERT (ID-Cert, 2017) spam (upaya pengiriman pesan secara beruntun tanpa dikehendaki oleh pihak penerima) merupakah kasus terbanyak sepanjang tahun 2017. Selanjutnya, ID-Cert juga melaporkan bahwa telah terjadi *phising* (pencurian identitas pengguna pada saat melakukan login di situs palsu) di sebuah situs sekolah di Indonesia terkait login palsu ke universitas di luar negeri.

Peristiwa yang terjadi baik pada institusi pendidikan secara global maupun kondisi keamanan informasi di Indonesia perlu menjadi perhatian bagi para pelaku penyelenggara institusi pendidikan di Indonesia. Hal tersebut dikarenakan mayoritas institusi pendidikan sudah mulai memanfaatkan teknologi informasi (TI). Salah satu bentuk pemanfaatan TI di institusi pendidikan, yaitu adanya system pembelajaran elektronik atau biasa disebut dengan elearning. Elearning merupakan suatu metode pembelajaran menggunakan perangkat elektronik dan media digital (Chistensson, 2017).

Berbagai institusi Pendidikan di Indonesia umunya telah memiliki system pusat teknologi informasi dan pangkalan data (PTIPD). Universitas Islam Negri Sunan Kalijaga Yogyakarta merupakan salah satu perguruan tinggi yang telah memiliki unit pelaksana teknis dalam bidang pusat teknologi dan pangkalan data mengingat seiring dengan perkembangan teknologi yang menuntut adanya jaminan pengelolaan data dan pengolahan serta penyajian informasi yang cepat dan akurat, maka pada tahun 2013 diadakan perubahan tugas dan fungsi dari Pusat Computer Dan System Informasi PKSI yang berdampak pada perubahan terhadap nama unit pengelola data dan informasi ini sehingga menjadi Pusat Teknologi Informasi dan Pangkalan Data (PTIPD). Kebutuhan terhadap perubahan ini terjadi secara umum di tingkat nasional, sehingga nama, tugas, dan fungsi dari unit pelaksana pengelola data dan teknologi informasi ini dibuat standar untuk seluruh Perguruan Tinggi Agama Islam Negeri (PTAIN) (PTIPD UIN Sunan Kalijaga, 2022).

Sebagai bentuk implementasi undang-undang yang berlaku pihak Kementrian Komunikasi dan Informatika (Kemkominfo) Republik Indonesia mengharapkan organisasi yang menyelenggarakan sistem elektronik dapat melakukan sertifikasi SNI ISO 27001 terkait keamanan informasi. Kondisi organisasi yang akan melakukan sertifikasi diharapkan berada pada tingkat kematangan III+ (Tim Direktorat Keamanan Informasi, 2011). Dengan kata lain, terdapat suatu gap antara kondisi yang diharapkan dengan kondisi sebenarnya. Oleh sebab itu, perlu dilakukan penilaian terkait dengan sejauh mana penerapan keamanan informasi di suatu organisasi atau instansi.

Ada beberapa alat penilaian yang dapat digunakan terkait keamanan informasi di institusi Pendidikan diantaranya dapat menggunakan Indeks Keamanan Informasi (KAMI) yang digunakan sebagai alat penilaian yang disusun oleh Kementrian Komunikasi dan Informatika (Kemkominfo) Republik Indonesia.

Penggunaan indeks KAMI versi 4.2 didasarkan atas SNI ISO 27001:2013. Terdapat 7 komponen di dalam indeks KAMI versi 4.2, yaitu: system elektronik (SE), tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja pengelolaan keamanan informasi, pengelolaan asset informasi, jenis teknologi dan pengamanan pihak ketiga (suplemen). Pada penelitian ini akan berfokus pada analisis dan evaluasi dari sector suplemen pada bagian ke 7 yang meliputi evaluasi kesiapan pengamanan keterlibatan pihak ketiga, pengamanan layanan infrastrukutur awan dan perlindungan data pribadi. Hal itu mengakibatkan perlu adanya perhatian khusus terkait dengan sector suplemen yang meliputi 3 area yang sudah di sebutkan didiatas. Oleh sebab itu, penting untuk melakukan penilaian atas pengamanan teknologi yang telah dilakukan.

2. TINJAUAN PUSTAKA

2.1. Informasi Sebagai Aset

Menurut (Hutahaean, J., 2015)terdapat lima jenis utama sumber daya, yaitu man (sumber daya manusia), material (sumber daya material), machine (sumber daya peralatan termasuk fasilitas dan energi), money (sumber daya keuangan), dan information (sumber daya informasi termasuk data). Sumber daya manusia, material, dan keuangan tergolong dalam sumber daya fisik karena sumber-sumber tersebut memiliki wujud secara fisik, sedangkan sumber daya informasi tergolong dalam sumber daya konseptual karena sumber daya tersebut memiliki nilai dari apa yang diwakilinya.

2.2. Keamanan Informasi

Keamanan informasi merupakan suatu upaya untuk mengamankan aset informasi terhadap ancaman yang mungkin akan timbul. Sehingga keamanan informasi secara tidak langsung dapat menjamin kontinuitas bisnis, mengurangi resikoresiko yang terjadi, dan mengoptimalkan pengembalian investasi. Semakin banyak informasi perusahaan yang disimpan, dikelola dan disharingkan maka semakin besar pula resiko terjadi kerusakan, kehilangan atau terekspos nya data ke pihak eksternal yang tidak diinginkan.

Keamanan informasi merupakan aspek penting dalam usaha melindungi aset informasi dalam sebuah organisasi. Menurut (Whitman, M.E. and Mattord, 2021) Jenis keamanan informasi dapat dibagi menjadi beberapa bagian berikut: Physical security, Personal security , Operational security, Communications security, Network security.

Informasi merupakan salah satu aset penting dari perusahaan. Perusahaan melakukan pengolahan terhadap informasi, kemudian hasilnya disimpan dan dibagikan. Menurut (Harliana, P., Perdana, A. and Prasetyo, R.M., 2015) Keamanan sistem informasi terdiri dari perlindungan terhadap aspek-aspek berikut ini:

1. *Confidentiality* (Kerahasiaan) Aspek yang menjamin kerahasian data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasian data yang dikirim, diterima dan disimpan.
2. *Integrity* (Integritas) Aspek yang menjamin bahwa data tidak diubah tanpa ada ijin pihak yang berwenang (authorized), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini.
3. *Availability* (Ketersediaan) Aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait.

2.3. Sistem Manajemen Keamanan Informasi

Sebuah organisasi harus menerapkan Sistem Manajemen Keamanan Informasi untuk menjamin keamanan aset teknologi informasi dan komunikasi (TIK). Sistem Manajemen Keamanan Informasi adalah kumpulan dari kebijakan dan prosedur untuk mengatur data sensitif milik organisasi secara sistematis. Tujuan dari SMKI sendiri adalah untuk meminimalisir risiko dan menjamin kelangsungan bisnis secara proaktif untuk membatasi dampak dari pelanggaran keamanan.

Sistem Manajemen Keamanan Informasi juga harus mengacu pada standar nasional atau internasional yang ada agar kualitas pengamanan yang diberikan tinggi dan mampu menanggulangi adanya masalah. Standar internasional yang telah direkomendasikan untuk penerapan SMKI adalah ISO/IEC 27001. Standar ini telah berjalan berbasis risiko sehingga mampu mengurangi ancaman dan menanggulangi masalah dengan cepat dan tepat.

2.4. Ruang Lingkup Area Suplemen Dalam Indeks KAMI Versi 4.2

Perkembangan teknologi yang pesat dan pola bisnis yang dinamis menyebabkan munculnya risiko keamanan informasi baru. Keterlibatan pihak ketiga dalam rantai pasok *(supply chain)* layanan suatu instansi/perusahaan menimbulkan risiko terkait keberadaan/keterlibatan pihak eksternal tersebut. Layanan berbasis infrastruktur awan *(Cloud)* memberikan peluang efisiensi dan peningkatan kinerja yang sangat signifikan bagi instansi/perusahaan, akan tetapi risiko terkait data yang berada pada pengendalian pihak ketiha (penyelenggara layanan) perlu dimitgasi.

Sedangkan disahkannya peraturan terkait perlindungan data pribadi oleh banyak negara

memerlukan kerangka kerja yang secara spesifik membahas bagaimana data pribadi yang ada/digunakan dalam instansi/perusahaan diamankan sesuai dengan persyaratan hukum (Badan Siber dan Sandi Negara, 2022).

Bagian area VII Suplemen akan mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi. Berilah tanda *checklist* untuk jawaban yang sesuai dengan kondisi yang ada di instansi dan isi sesuai dengan tingkat kepentingan yaitu:

a. 0 = Tidak dilakukan
b. 1 = Dalam perencanaan
c. 2 = Dalam Penerapan / Diterapkan sebagian
d. 3 = Diterapkan secara menyeluruh

1. Penilaian Pengamanan keterlibatan pihak ketiga penyedia layanan, sebagaimana terdapat pada gambar 1

No	Fungsi/Organisasi Kemanan Informasi	Status			
		0	1	2	3
7.1	**Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan**				
7.1.1	**Manajemen Risiko dan Pengelolaan Keamanan pihak ketiga**				
7.1.1.1	Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?				
7.1.1.2	Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?				
7.1.1.3	Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?				
7.1.1.4	Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?				
7.1.1.5	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?				
7.1.1.6	Apakah kebijakan tersebut (7.1.1.5) telah dikomunikasikan kepada pihak ketiga dan mereka menyatakan persetujuannya dalam dokumen kontrak, SLA atau dokumen sejenis lainnya?				
7.1.1.7	Apakah hak audit TI secara berkala ke pihak ketiga/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/pihak ketiga?				
7.1.2	**Pengelolaan Sub-Kontraktor/Alih Daya pada Pihak Ketiga**				
7.1.2.1	Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan dalam layanannya?				
7.1.2.2	Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?				
7.1.2.3	Apakah pihak ketiga melakukan pemantauan dan evaluasi terhadap kepatuhan alih daya, subkontraktor atau penyedia teknologi/infrastruktur terhadap persyaratan keamanan yang ditetapkan?				
7.1.3	**Pengelolaan Layanan dan Keamanan Pihak Ketiga**				
7.1.3.1	Apakah instansi/perusahaan telah menetapkan proses, prosedur atau rencana terdokumentasi untuk mengelola dan memantau layanan dan aspek keamanan informasi (termasuk pengamanan aset informasi dan infrastruktur milik instansi/perusahaan yang diakses) dalam hubungan kerjasama dengan pihak ketiga?				
7.1.3.2	Apakah peran dan tanggung jawab pemantauan, evaluasi dan/atau audit aspek keamanan informasi pihak ketiga telah ditetapkan dan/atau ditugaskan dalam unit organisasi tertentu?				
7.1.3.3	Apakah tersedia laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian komersil (kontrak)?				
7.1.3.4	Apakah ada rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan?				
7.1.3.5	Apakah hasil pemantauan dan evaluasi terhadap laporan atau pembahasan dalam rapat berkala tersebut didokumentasikan, dikomunikasikan dan ditindaklanjuti oleh pihak ketiga serta dilaporkan kemajuannya kepada instansi/perusahaan?				
7.1.3.6	Apakah instansi/perusahaan telah menetapkan rencana dan melakukan audit terhadap pemenuhan persyaratan keamanan informasi oleh pihak ketiga?				
7.1.3.7	Apakah hasil audit tersebut ditindaklanjuti oleh pihak ketiga dengan melaporkan rencana perbaikan yang terukur dan bukti-bukti penerapan rencana tersebut?				
7.1.3.8	Apakah kondisi terkait denda / penalti karena ketidakpatuhan pihak ketiga terhadap persyaratan dan / atau tingkat layanan telah didokumentasikan, dikomunikasikan, dipahami dan diterapkan?				
7.1.4	**Pengelolaan Perubahan Layanan dan Kebijakan Pihak Ketiga**				
7.1.4.1	Apakah instansi/perusahaan mengelola perubahan yang terjadi dalam hubungan dengan pihak ketiga yang menyangkut antara lain? - Perubahan layanan pihak ketiga; - Perubahan kebijakan, prosedur, dan/atau - Kontrol risiko pihak ketiga?				
7.1.4.2	Apakah risiko yang menyertai perubahan tersebut dikaji, didokumentasikan dan ditetapkan rencana mitigasi barunya?				
7.1.5	**Penanganan Aset**				
7.1.5.1	Apakah pihak ketiga memiliki prosedur formal untuk menangani data selama dalam siklus hidupnya mulai dari pembuatan, pendaftaran, perubahan, dan penghapusan / penghancuran aset?				
7.1.5.2	Apakah per untuk penghancuran (disposal) data secara aman telah disepakati bersama pihak ketiga (pihak ketiga)?				
7.1.6	**Pengelolaan Insiden oleh Pihak Ketiga**				
7.1.6.1	Apakah pihak ketiga memiliki prosedur untuk pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi?				
7.1.6.2	Apakah pihak ketiga memiliki bukti-bukti penerapan yang memadai dalam menangani insiden keamanan informasi?				
7.1.7	**Rencana Kelangsungan Layanan Pihak Ketiga**				
7.1.7.1	Apakah pihak ketiga memiliki kebijakan, prosedur atau rencana terdokumentasi untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat/bencana?				
7.1.7.2	Apakah kebijakan, prosedur atau rencana kelangsungan layanan tersebut telah diujicoba, didokumentasikan hasilnya dan dievaluasi efektivitasnya?				
7.1.7.3	Apakah pihak ketiga memiliki organisasi atau tim khusus yang ditugaskan untuk mengelola proses kelangsungan layanannya?				

Gambar 1. Penilaian Indeks KAMI 4.2

1. Penilaian Pengamanan Infrastruktur awan *(Cloud)*, sebagaimana terdapat pada gambar 2

No	Fungsi/Organisasi Kemanan Informasi	Status			
		0	1	2	3
7.2	**Pengamanan Layanan Infrastruktur Awan (*Cloud Service*)**				
7.2.1	Apakah instansi/perusahaan sudah melakukan kajian risiko terkait penggunaan layanan berbasis *cloud* dan menyesuaikan kebijakan keamanan informasi terkait layanan ini?				
7.2.2	Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis *cloud*?				
7.2.3	Apakah instansi/perusahaan sudah menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan *cloud*?				
7.2.4	Apakah instansi/perusahaan sudah mengkaji, menetapkan kriteria dan memastikan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis *cloud*?				
7.2.5	Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan *cloud* terkait reputasi penyelenggaranya?				
7.2.6	Apakah instansi/perusahaan sudah menetapkan standar keamanan teknis penggunaan layanan *cloud*, termasuk aspek penggunaannya oleh pengguna di internal instansi/perusahaan?				
7.2.7	Apakah instansi/perusahaan sudah mengevaluasi kelaikan keamanan layanan *cloud* termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO 27001?				
7.2.8	Apakah instansi/perusahaan sudah memiliki kebijakan, strategi dan proses untuk mengganti layanan *cloud* atau menyediakan fasilitas pengganti apabila terjadi gangguan sementara pada layanan tersebut?				
7.2.9	Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan *cloud*?				
7.2.10	Apakah instansi/perusahaan sudah memiliki proses untuk menghentikan layanan *cloud*, termasuk proses pengamanan data yang ada (memindahkan dan menghapus data)?				

Gambar 2 Penilaian Indeks KAMI 4.2

2. Penilaian Pengamanan perlindungan data pribadi, sebagaimana terdapat pada gambar 3

No	Fungsi/Organisasi Kemanan Informasi	Status			
		0	1	2	3
7.3	**Perlindungan Data Pribadi**				
7.3.1	Apakah instansi/perusahaan sudah mendokumentasikan jenis dan bentuk (dokumen kertas/elektronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal?				
7.3.2	Apakah instansi/perusahaan sudah memetakan alur pemrosesan data di internal dan pertukaran data dengan pihak eksternal, termasuk kapan dan dimana data pribadi tersebut diperoleh?				
7.3.3	Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan?				
7.3.4	Apakah instansi/perusahaan sudah memiliki kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku?				
7.3.5	Apakah instansi/perusahaan sudah menunjuk pejabat-pejabat (*Data Protection Officer, Data Controller, Data Processor*) yang bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Perlindungan Data Pribadi?				
7.3.6	Apakah instansi/perusahaan sudah menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain?				
7.3.7	Apakah kajian risiko keamanan pada instansi/perusahaan sudah memasukkan aspek Perlindungan Data Pribadi?				
7.3.8	Apakah mekanisme perlindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku?				
7.3.9	Apakah instansi/perusahaan sudah menjalankan program peningkatan pemahaman/kepedulian kepada seluruh pegawai terkait Perlindungan Data Pribadi, termasuk hal-hal terkait Peraturan Perundangan yang berlaku?				
7.3.10	Apakah instansi/perusahaan sudah mendapatkan persetujuan dari pemilik data pribadi saat mengambil data tersebut, termasuk penjelasan hak pemilik data, apa saja yang akan diberlakukan pada data pribadi tersebut dan menyimpan catatan persetujuan tersebut ?				
7.3.11	Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi?				
7.3.12	Apakah instansi/perusahaan sudah menerapkan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut?				
7.3.13	Apakah instansi/perusahaan sudah menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan termutakhirkan?				
7.3.14	Apakah instansi/perusahaan sudah menerapkan proses terkait periode penyimpanan data pribadi dan penghapusan/pemusnahannya sesuai dengan peraturan atau perjanjian dengan pemilik data?				
7.3.15	Apakah instansi/perusahaan sudah menerapkan proses terkait penghapusan/pemusnahan data apabila sudah tidak ada keperluan yang sah untuk menyimpan/mengolahnya lebih lanjut atau atas permintaan pemilik data dan menyimpan catatan proses tersebut?				
7.3.16	Apakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?				

Gambar 3 Penilaian Indeks KAMI 4.2

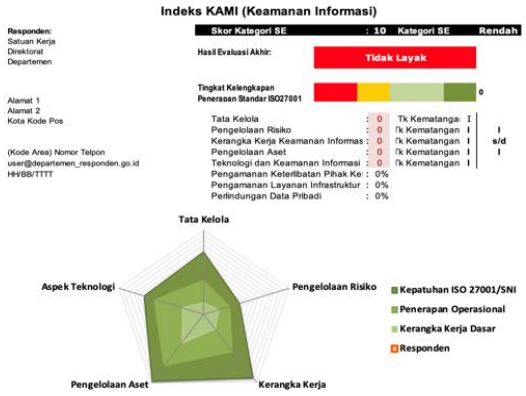
2.5. Indeks Keamanan Informasi (KAMI) 4.2

Indeks KAMI versi 4.2 adalah sebuah tools yang digunakan untuk mengevaluasi tingkat kematangan, tingkat kelengkapan penerapan ISO 27001:2013 dan gambaran tata kelola keamanan informasi di sebuah organisasi. Indeks KAMI ini dibuat oleh pihak Kementrian Kominfo. Alat evaluasi ini tidak digunakan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat yang untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pemimpin instansi.

Alat evaluasi Indeks KAMI dianjurkan untuk dilakukan oleh pejabat yang secara langsung bertanggung jawab dan berwenang untuk mengelola keamanan informasi di seluruh cakupan instansinya. Evaluasi yang dilakukan dengan menggunakan indeks KAMI ini mencakup 7 target area, yaitu sistem elektronik, tata kelola keamanan informasi, risiko keamana informasi, kerangka kerja pengelolaan informasi, pengelolaan aset informasi, teknologi dan keamanan informasi, dan suplemen yang meliputi 3 aspek yaitu: pengamanan keterlibatan pihak ketiga

mendapatkan, pengamanan layanan infrastruktur awan *(cloud)* dan untuk pengamanan perlindungan data pribadi.

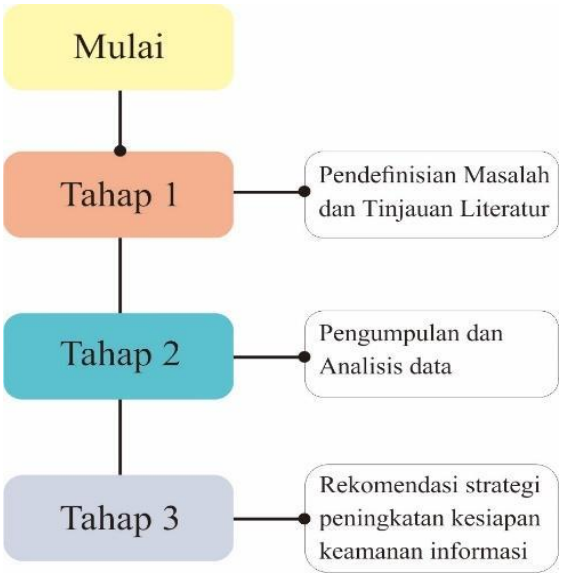
Hasil penilaian menggunakan Indeks KAMI versi 4.2 akan digambarkan kedalam diagram yang berbentuk jaring laba-laba (*spider chart*) dengan 7 area utama. Dalam jaring laba-laba tersebut juga akan dilihat tentang nilai Indeks KAMI dengan kepatuhan terhadap ISO/IEC 27001:2013. Hasil penilaian evaluasi kesiapan Pengamanan Keterlibatan Pihak Ketiga, Pengamanan Layanan Infrastrukutur Awan dan Perlindungan Data Pribadi disampaikan dalam bentuk persentase (%) dengan obyektif atau sasaran pencapaian maksimal. dapat dilihat melalui gambar 4 sebagai berikut :



Gambar 4 Dashboard Indeks KAMI Versi 4.2

3. METODOLOGI

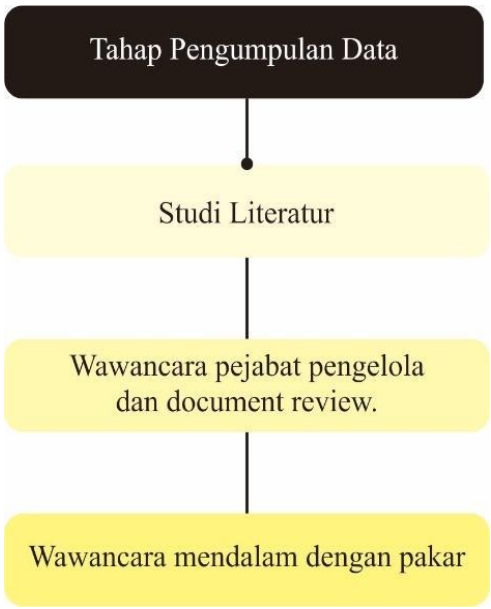
Penelitian ini adalah penelitian evaluatif mengenai kesiapan penerapan tata kelola keamanan informasi dengan metode penelitian kualitatif. Tujuan penelitian ini adalah untuk menghasilkan sebuah rekomendasi terkait dengan pengamanan informasi terkaiat keterlibatan pihak eksternal penyedia layanan cloud dan perlindungan data pribadi pengguna.



Gambar 5. Tahap Penelitian

Gambar 5 merupakan masing-masing tahapan penelitian secara sistematis dijelaskan pada penjelasan berikut:

1. **Tahap 1**, pendefinisian masalah dan tinjauan literatur. Pada tahap ini dilakukan untuk mempelajari berbagai teori yang relevan mencakup teori untuk mengkaji kesiapan pengamanan informasi instansi terkait pengamanan informasi terkaiat keterlibatan pihak eksternal penyedia layanan cloud dan perlindungan data pribadi pengguna
2. **Tahap 2**, pengumpulan dan analisis data. Setelah diperoleh model pengkajian yang cocok, dilakukan pengumpulan data berikut analisis data untuk mengetahui kondisi kesiapan pengamanan informasi pada instansi.
3. **Tahap 3**, rekomendasi strategi peningkatan kesiapan keamanan informasi pada instansi. Berdasarkan data kondisi tersebut dilakukan *gap analysis* dengan kondisi ideal, selanjutnya akan disusun strategi dan alternatif kebijakan peningkatan kesiapan pengamanan informasi disuatu instansi yang befokus pada pengamanan informasi terkaiat keterlibatan pihak eksternal penyedia layanan cloud dan perlindungan data pribadi pengguna.



Gambar 6. Tahap Pengumpulan Data

Setelah melakukan pemetaan terkait tahap penelitian, kemudian peneliti melakukan dan membuat teknik pengumpulan data untuk dapat memberikan evaluasi dan analisis terhadap kondisi dan *checklist* data oleh pihak terkait, seperti yang diperlihatkan pada gambar 6. Adapun tahap analisis data sebagai berikut:

1. **Studi Literatur.** Studi literatur dilakukan untuk mempelajari berbagai dokumen/ referensi yang

terkait dengan tema penelitian untuk dijadikan acuan.

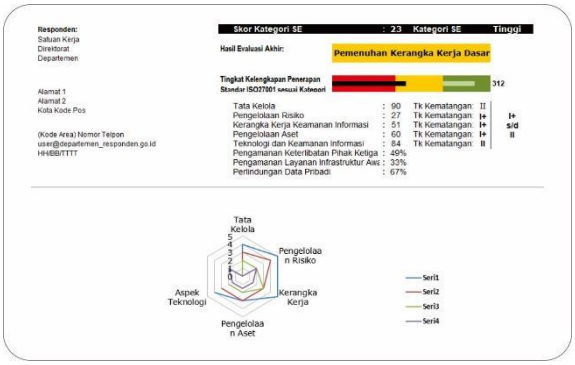
2. **Wawancara pejabat pengelola dan document review.** Proses ini dilakukan untuk mendapatkan gambaran terkini/kondisi mengenai objek penelitian. Dalam penelitian ini, proses ini dilakukan juga untuk mengetahui visimisi, strategi serta tujuan jangka panjang keamanan informasi pemerintah.
3. **Wawancara mendalam dengan pakar.** Wawancara dengan pakar bertujuan untuk mendapatkan pandangan dari pakar secara teknis mengenai kondisi kesiapan keamanan informasi.

Analisis dan interpretasi data menggunakan metode analisis kualitatif. Teknik analisis ini dilakukan menggunakan pendekatan logika induktif, di mana penarikan kesimpulan dibangun berdasarkan pada hal-hal khusus atau data di lapangan yang bermuara pada kesimpulan- kesimpulan umum. Analisis data kualitatif adalah upaya yang dilakukan dengan cara mengorganisasikan data dengan memilah-milahnya menjadi satuan yang dapat dikelola kemudian (BOGDAN, 1998). Kemudian berdasarkan proses tersebut, ditemukan apa yang penting dan apa yang dapat dipelajari untuk menunjang keputusan. Penelitian ini dilakukan di pusat teknologi informasi dan pangkalan data (PTIPD) Universitas Islam Negri Sunan Kalijaga Yogyakarta.

4. HASIL DAN PEMBAHASAN

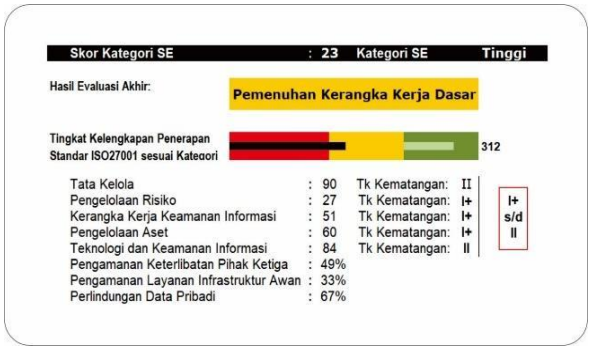
4.1. Analisis Hasil Penilaian Indeks KAMI

Gambar 7 adalah tampilan dashboard penilaian menggunakan indeks keamanan informasi (KAMI) versi 4.2 pada instansi pendidikan di Kantor Pusat Informasi dan pangkalan data (PTIPD) UIN Sunan Kalijaga Yogyakarta.



Gambar 7. Hasil Dashboard Indeks KAMI versi 4.2 di PTIPD UIN Sunan Kalijaga Yogyakarta

Dashboard diatas merupakan gambaran secara keseluruhan dari penilaian yang telah dilakukan dengan menggunakan indeks KAMI versi 4.2. Dari dashboard diatas, dapat dilihat bahwa tingkat kematangan keamanan informasi di Kantor Pusat Teknologi Informasi dan Pangkalan Data (PTIPD) UIN Sunan Kalijaga Yogyakarta masih berada pada tingkat II dengan nilai sebesar 312. Dapat dilihat pada radar chart dashboard tersebut bahwa hampir seluruh area yang dinilai dalam indeks KAMI belum terpenuhi dan sesuai dengan ISO 27001. Jika dilihat dibagian radar chart dashboard hasil yang didapat sampai kategori proses penerapan.



Gambar 8. Hasil Penilaian Indeks KAMI versi 4.2 di PTIPD UIN Sunan Kalijaga Yogyakarta

Untuk tingkat kematangan setiap area yang telah dinilai dalam indeks KAMI versi 4.2 masih masih berada pada kategori I+ dan II.Pada tabel 1 Berikut adalah uraian dari tingkat kematangan kelima area yang telah dinilai sebelumnya:

Tabel 1. Tingkat Kematangan Keamana Informasi PTIPD UIN Sunan Kalijaga Menggunakan Indeks KAMI Versi 4.2

	Tata kelola	Pengelola-an resiko	Kerangka kerja	Pengelola-an aset	Tekno-logi
Tingkat Kematangan II					
Status	II	I+	I+	II	II
Tingkat Kematangan III					
Status	No	No	No	No	No
Validitas	No	No	No	No	No
Tingkat Kematangan IV					
Status	No	No	No	No	No
Validitas	No	No	No	No	No
Tingkat Kematangan V					
Status	No	No	No	No	No
Validitas	No	No	No	No	No
Status Akhir	II	I+	I+	I+	II

Urutan tingkat kematangan dari yang terendah hingga yang tertinggi adalah I – V. Batasan minimal yang harus dicapai agar dapat melakukan sertifikasi ISO adalah III+, sedangkan untuk saat ini tingkat kematangan dari Kantor Pusat Teknologi Informasi dan Pangkalan Data (PTIPD) UIN Sunan Kalijaga Yogyakarta berada pada tingkat I - II. Tingkat kematangan ini menunjukkan posisi Kantor PTIPD UIN Sunan Kalijaga Yogyakarta sebagai mana yang diperlihatkan pada tabel 2.

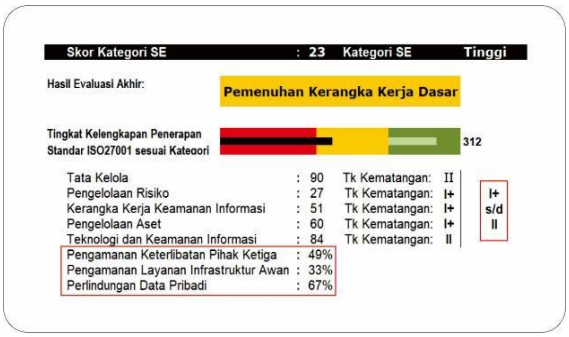
Tabel 2. Tingkat Kondisi Kematangan Keamana Informasi PTIPD UIN Sunan Kalijaga

Tingkatan	Kondisi
I	Kondisi Awal
II	Penerapan Kerangka Kerja Dasar
III	Terdefinisi dan Konsisten
IV	Terkelola dan Terukur
V	Optimal

4.2. Hasil Pengisian Kuesioner Indeks KAMI

Hasil dari evaluasi tingkat presentase kelengkapan dan efektifitas penggunaan teknologi dalam pengamanan aset informasi di PTIPD UIN Sunan Kalijaga Yogyakarta yaitu: untuk pengamanan keterlibatan pihak ketiga mendapatkan presentase 49%, pengamanan layanan infrastruktur awan *(cloud)* sebesar 33% dan untuk pengamanan perlindungan data pribadi mendapatkan presentase 67%. Rekomendasi dari penelitian ini dapat di jadikan sebagai bahan pertimbangan dan evaluasi bagi instansi dalam melakukan perbaikan yang berkaitan dengan mitigasi risiko dan pencegahan terhadap kerentanan keamanan informasi, serta dapat memastikan aturan dapat tercapai dengan baik dan keputusan terhadap kebijakan keamanan informasi dalam satu instansi di masa depan.

Terlihat pada gambar 9 untuk kategori Suplemen yang meliputi 3 area tersebut memiliki tingkat kondisi keamanan yang sangat rendah, oleh karena itu instansi tersebut harus segera melakukan perbaikan dan mitigasi risiko yang diperlukan untuk mencegah hal-hal yang tidak di ingingkan di masa depan.



Gambar 9 Hasil presentase Tingkat Pengamanan Pihak Eksternal, Layanan Infrastruktur Awan dan Perlindungan Data Pribadi

1. Hasil *checklist* Bagian VII Suplemen terkait pengamanan informasi pihak ketiga (eksternal) menggunakan indeks KAMI Versi 4.2 dengan simbol *checklist* pada tabel 3 sebagai berikut:

Tabel 3. Hasil pengisian kuesioner indeks KAMI versi 4.2 untuk kategori pengamanan pihak ketiga (ekternal) dalam pengamanan informasi.

No	Fungsi/Organisasi Kemanan Informasi	Status			
		0	1	2	3
7.1.1	Manajemen Risiko dan Pengelolaan Keamanan pihak ketiga				
7.1.1.1	Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?			✔	
7.1.1.2	Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?			✔	
7.1.1.3	Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?				✔
7.1.1.4	Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?				✔
7.1.1.5	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?				✔
7.1.1.6	Apakah kebijakan tersebut (7.1.1.5) telah dikomunikasikan kepada pihak ketiga dan mereka menyatakan persetujuannya dalam dokumen kontrak, SLA atau dokumen sejenis lainnya?				✔
7.1.1.7	Apakah hak audit TI secara berkala ke pihak ketiga/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/pihak ketiga?			✔	
7.1.2	Pengelolaan Sub-Kontraktor/Alih Daya pada Pihak Ketiga				
7.1.2.1	Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan dalam layanannya?			✔	
7.1.2.2	Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?				✔
7.1.2.3	Apakah pihak ketiga melakukan pemantauan dan evaluasi terhadap kepatuhan alih daya, subkontraktor atau penyedia teknologi/infrastruktur terhadap persyaratan keamanan yang ditetapkan?				✔
7.1.3	Pengelolaan Layanan dan Keamanan Pihak Ketiga				
7.1.3.1	Apakah instansi/perusahaan telah menetapkan proses, prosedur atau rencana terdokumentasi untuk mengelola dan memantau layanan dan aspek keamanan informasi (termasuk pengamanan aset informasi dan infrastruktur milik instanasi/perusahaan yang diakses) dalam hubungan kerjasama dengan pihak ketiga?			✔	
7.1.3.2	Apakah peran dan tanggung jawab pemantauan, evaluasi dan/atau audit aspek keamanan informasi pihak ketiga telah ditetapkan dan/atau ditugaskan dalam unit organisasi			✔	

No	Fungsi/Organisasi Kemanan Informasi	Status			
		0	1	2	3
	tertentu?				
7.1.3.3	Apakah tersedia laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian komersil (kontrak)?			✔	
7.1.3.4	Apakah ada rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan?			✔	
7.1.3.5	Apakah hasil pemantauan dan evaluasi terhadap laporan atau pembahasan dalam rapat berkala tersebut didokumentasikan, dikomunikasikan dan ditindaklanjuti oleh pihak ketiga serta dilaporkan kemajuannya kepada instansi/perusahaan?			✔	
7.1.3.6	Apakah instansi/perusahaan telah menetapkan rencana dan melakukan audit terhadap pemenuhan persyaratan keamanan informasi oleh pihak ketiga?			✔	
7.1.3.7	Apakah hasil audit tersebut ditindaklanjuti oleh pihak ketiga dengan melaporkan rencana perbaikan yang terukur dan bukti-bukti penerapan rencana tersebut?			✔	
7.1.3.8	Apakah kondisi terkait denda / penalti karena ketidakpatuhan pihak ketiga terhadap persyaratan dan / atau tingkat layanan telah didokumentasikan, dikomunikasikan, dipahami dan diterapkan?			✔	
7.1.4	Pengelolaan Perubahan Layanan dan Kebijakan Pihak Ketiga				
7.1.4.1	Apakah instansi/perusahaan mengelola perubahan yang terjadi dalam hubungan dengan pihak ketiga yang menyangkut antara lain? - Perubahan layanan pihak ketiga; - Perubahan kebijakan, prosedur, dan/atau - Kontrol risiko pihak ketiga?			✔	
7.1.4.2	Apakah risiko yang menyertai perubahan tersebut dikaji, didokumentasikan dan ditetapkan rencana mitigasi barunya?			✔	
7.1.5	Penanganan Aset				
7.1.5.1	Apakah pihak ketiga memiliki prosedur formal untuk menangani data selama dalam siklus hidupnya mulai dari pembuatan, pendaftaran, perubahan, dan penghapusan / penghancuran aset?			✔	
7.1.5.2	Apakah per untuk penghancuran (disposal) data secara aman telah disepakati bersama pihak ketiga (pihak ketiga)?			✔	
7.1.6	Pengelolaan Insiden oleh Pihak Ketiga				
7.1.6.1	Apakah pihak ketiga memiliki prosedur untuk pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi?			✔	
7.1.6.2	Apakah pihak ketiga memiliki bukti-bukti penerapan yang memadai dalam menangani insiden keamanan informasi?			✔	
7.1.7	Rencana Kelangsungan Layanan Pihak Ketiga				
7.1.7.1	Apakah pihak ketiga memiliki kebijakan, prosedur atau rencana terdokumentasi untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat/bencana?				✔
7.1.7.2	Apakah kebijakan, prosedur atau rencana kelangsungan layanan tersebut telah diujicoba, didokumentasikan hasilnya dan dievaluasi efektivitasnya?				✔
7.1.7.3	Apakah pihak ketiga memiliki organisasi atau tim khusus yang ditugaskan untuk mengelola proses kelangsungan layanannya?				✔

2. Hasil *checklist* Bagian VII Suplemen terkait pengamanan layanan infrasttruktur awan *(cloud)* menggunakan indeks KAMI Versi 4.2 dengan simbol *checklist* pada tabel 4, sebagai berikut:

Tabel 4. Hasil pengisian kuesioner indeks KAMI versi 4.2 untuk area pengamanan layanan infrasttruktur awan (cloud).

No	Fungsi/Organisasi Kemanan Informasi	Status			
		0	1	2	3
7.2.1	Apakah instansi/perusahaan sudah melakukan kajian risiko terkait penggunaan layanan berbasis *cloud* dan menyesuaikan kebijakan keamanan informasi terkait layanan ini?				
7.2.2	Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis *cloud*?			✔	
7.2.3	Apakah instansi/perusahaan sudah menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan *cloud*?			✔	
7.2.4	Apakah instansi/perusahaan sudah mengkaji, menetapkan kriteria dan memastikan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis *cloud*?			✔	
7.2.5	Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan *cloud* terkait reputasi penyelenggaranya?			✔	
7.2.6	Apakah instansi/perusahaan sudah menetapkan standar keamanan teknis penggunaan layanan *cloud*, termasuk aspek penggunaannya oleh pengguna di internal instansi/perusahaan?			✔	
7.2.7	Apakah instansi/perusahaan sudah mengevaluasi kelaikan keamanan layanan *cloud* termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO			✔	

No	Fungsi/Organisasi Kemanan Informasi	Status			
		0	1	2	3
	27001?				
7.2.8	Apakah instansi/perusahaan sudah memiliki kebijakan, strategi dan proses untuk mengganti layanan *cloud* atau menyediakan fasilitas pengganti apabila terjadi gangguan sementara pada layanan tersebut?			✔	
7.2.9	Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan *cloud*?				
7.2.10	Apakah instansi/perusahaan sudah memiliki proses untuk menghentikan layanan *cloud*, termasuk proses pengamanan data yang ada (memindahkan dan menghapus data)?			✔	

3. Hasil *checklist* Bagian VII Suplemen terkait perlindungan data pribadi menggunakan indeks KAMI Versi 4.2 dengan simbol *checklist* pada tabel 5, sebagai berikut:

Tabel 5. Hasil pengisian kuesioner indeks KAMI versi 4.2 untuk area perlindungan data pribadi pengguna

No	Fungsi/Organisasi Kemanan Informasi	Status			
		0	1	2	3
7.3.1	Apakah instansi/perusahaan sudah mendokumentasikan jenis dan bentuk (dokumen kertas/elektronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal?				
7.3.2	Apakah instansi/perusahaan sudah memetakan alur pemrosesan data di internal dan pertukaran data dengan pihak eksternal, termasuk kapan dan dimana data pribadi tersebut diperoleh?			✔	
7.3.3	Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan?			✔	
7.3.4	Apakah instansi/perusahaan sudah memiliki kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku?			✔	
7.3.5	Apakah instansi/perusahaan sudah menunjuk pejabat-pejabat (*Data Protection Officer, Data Controller, Data Processor*) yang bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Perlindungan Data Pribadi?			✔	
7.3.6	Apakah instansi/perusahaan sudah menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain?				✔
7.3.7	Apakah kajian risiko keamanan pada instansi/perusahaan sudah memasukkan aspek Perlindungan Data Pribadi?				✔
7.3.8	Apakah mekanisme perlindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku?				✔
7.3.9	Apakah instansi/perusahaan sudah menjalankan program peningkatan pemahaman/kepedulian kepada seluruh pegawai terkait Perlindungan Data Pribadi, termasuk hal-hal terkait Peraturan Perundangan yang berlaku?				
7.3.10	Apakah instansi/perusahaan sudah mendapatkan persetujuan dari pemilik data pribadi saat mengambil data tersebut, termasuk penjelasan hak pemilik data, apa saja yang akan diberlakukan pada data pribadi tersebut dan menyimpan catatan persetujuan tersebut ?				✔
7.3.11	Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi?				✔
7.3.12	Apakah instansi/perusahaan sudah menerapkan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut?				✔
7.3.13	Apakah instansi/perusahaan sudah menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan termutakhirkan?				✔
7.3.14	Apakah instansi/perusahaan sudah menerapkan proses terkait periode penyimpanan data pribadi dan penghapusan/pemusnahannya sesuai dengan peraturan atau perjanjian dengan pemilik data?				✔
7.3.15	Apakah instansi/perusahaan sudah menerapkan proses terkait penghapusan/pemusnahan data apabila sudah tidak ada keperluan yang sah untuk menyimpan/mengolahnya lebih lanjut atau atas permintaan pemilik data dan menyimpan catatan proses tersebut?				✔
7.3.16	Apakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?				✔

Setelah pengisian kuesioner telah dilakukan pada bagian kategori VII Tentang suplemen yang meliputi 3 area diantaranya, pengamanan pihak ketiga (eksternal), pengamanan layanan infrastruktur awan *(cloud)* dan perlindungan data pribadi dengan hasil presentase penilaian seusai dengan indeks keamana informasi (KAMI) versi 4.3 maka di dapatkan hasil pada tabel 6, sebagai berikut:

Tabel 6. Hasil Presentase bagian VII Berdasarkan Indeks KAMI Versi 4.2

Area	Bagian VII Suplemen	Presentase % Indeks KAMI Versi 4.2
I	Pengamanan Informasi Pihak Ketiga (Eksternal)	49%
II	Pengamanan Layanan Infrastruktur Awan (Cloud)	33%
III	Perlindungan Data Pribadi	67%

4.3. Rekomendasi

Berdasarkan perhitungan kuisioner, analisis tiap area Indeks KAMI serta kondisi keamanan informasi saat ini pada PTIPD UIN Sunan Kalijaga Yogyakarta, maka untuk meningkatkan tingkat kematangan keamanan informasi sesuai dengan sertifikasi ISO 27001:2013 diperlukan rekomendasi-rekomendasi. Rekomendasi yang diberikan didasarkan oleh standar SNI ISO/IEC 27001:2013 dengan melakukan perbandingan antara hasil evaluasi Indeks KAMI versi 4.2 dan kontrol yang ada pada SNI ISO/IEC 27001:2013. Perbandingan yang dilakukan adalah dengan melihat kekurangan setiap area dan dibandingkan terhadap kontrol yang ada pada SNI ISO/IEC 27001:2013.

Tabel 7 berikut merupakan rekomendasi pada kategori pengamanan pihak ketiga (eksternal), pengamanan layanan infrastruktur awan *(cloud)* dan perlindungan data pribadi menggunakan indeks keamanan infromasi (KAMI) versi 4.2, sebagai berikut:

Tabel 7. Rekomendasi Pengamanan Informasi Terkait keterlibatan Pihak Ketiga (Eksternal) penyedia layanan cloud dan perlindungan data pribadi menggunakan ISO/IEC 27001di PTIPD UIN Sunan Kalijaga Yogyakarta

No	Kondisi *as-is*	Rekomendasi	Kontrol ISO 27001
1	Belum tersedia konfigurasi standar untuk keamanan sistem	Kebijakan kontrol akses mengenai konfigurasi keamanan sistem harus ditetapkan	A.9.1.1
2	Sistem belum mendukung penggantian password secara otomatis	Melakukan manajemen kata sandi	A.9.4.3
3	Belum memiliki standar untuk enskripsi	Membuat kebijakan tentang penggunaan kontrol kriptografi	A.10.1.1
4	Belum menerapkan pengamanan untuk mengelola kunci enkripsi	Melakukan pengelolaan kunci	A.10.1.2
5	Belum ada rekaman hasil pemutakhiran antivirus dan laporan penyerangan virus yang ditindaklanjuti	Melakukan kontrol terhadap malware	A.12.2.1
6	Perubahan dalam sistem informasi belum secara otomatis terekam di dalam log	Melakukan pencatatan kejadian yang merekam aktivitas	A.12.4.1
7	Belum ada sinkronisasi waktu yang akurat	Melakukan sinkronisasi waktu	A.12.4.4
8	Setiap aplikasi yang ada belum memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi	Melakukan analisis dan spesifikasi kebutuhan keamanan informasi	A.14.1.1
9	Belum mengamankan lingkungan pengembangan dan uji coba	Menerapkan lingkungan pengembangan yang aman	A.14.2.6
10	Belum secara rutin menganalisa kepatuhan penerapan konfigurasi standar	Melakukan peninjauan kepatuhan teknis	A.18.2.3

Rekomendasi dari penelitian ini dapat di jadikan sebagai bahan pertimbangan dan evaluasi bagi instansi dalam melakukan perbaikan yang berkaitan dengan mitigasi risiko dan pencegahan terhadap kerentanan keamanan informasi, serta dapat memastikan aturan dapat tercapai dengan baik dan keputusan terhadap kebijakan keamanan informasi dalam satu instansi di masa depan.

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Kesimpulan yang dapat diperoleh dari penelitian ini terkait penilaian manajemen keamanan informasi dengan menggunakan Indeks Keamanan Informasi (KAMI) versi 4.2 adalah sebagai berikut:

1. Hasil dari penilaian tingkat keamanan terkait pengamanan keterlibatan pihak ketiga mendapatkan presentase 49%, pengamanan layanan infrastruktur awan *(cloud)* sebesar 33% dan untuk pengamanan perlindungan data pribadi mendapatkan presentase 67%. Hal ini menunjukkan bahwa Pusat teknologi infromasi dan pangkalan data (PTIPD) UIN Sunan Kalijaga

masih memiliki banyak kekurangan dan perlu adanya perbaikan dan mitigasi risiko keamanan informasi.
2. Hasil keseluruhan dari penilaian ketujuh area dalam Indeks KAMI versi 4.2 adalah sebesar 312 dari jumlah total keseluruhan sebesar 645 dan berada pada level I-II dimana level ini berada pada kondisi awal penerapan keamanan informasi dan kondisi penerapan kerangka kerja dasar penerapan keamanan informasi.
3. Hasil analisis dan rekomendasi terkait evaluasi pengamanan keterlibatan pihak ketiga, pengamanan layanan infrastruktur awan *(cloud)* dan pengamanan perlindungan data pribadi ada 10 point yang disesuaikan dengan standart kontrol ISO/IEC 27001:2013

5.2. Rekomendasi dan Saran Perbaikan

Hasil analisis dari kuesioner Indeks KAMI versi 4.2 pada area ke 7 suplemen tentang pengamanan informasi dalam keterlibatan pihak eksternal, pengamanan infrastruktur awan (cloud) dan perlindungan data pribadi pengguna dapat diketahui kondisi yang menunjukan kekurangan dalam area ini.

Berdasarkan Tabel 4.6 rekomendasi yang diberikan kepada PTIPD UIN Sunan Kalijaga Yogyakarta sesuai dengan kontrol-kontrol yang ada dalam kontrol objektif 9.1, 9.4, 10.1, 12.2, 12.4, 14.1, 14.2, dan 18.2 pada ISO 27001:2013 untuk area pengamanan pihak eksternal, layanan infrastruktur awan dan perlindungan data pribadi; PTIPD UIN Sunan Kalijaga harus menetapkan, mendokumentasikan serta meninjau kebijakan kontrol akses berdasarkan persyaratan keamanan bisnis dan informasi, PTIPD harus membuat manajemen kata sandi yang interaktif dan harus memastikan kata sandi berkualitas, kemudian dalam kontrol enkripsi, kebijakan tentang penggunaan kontrol kriptografi untuk perlindungan informasi harus dikembangkan dan diimplementasikan serta mengembangkan dan menerapkan kebijakan tentang penggunaan, perlindungan, dan masa pakai kunci kriptografi melalui seluruh life *cycle*-nya, untuk kontrol terhadap malware PTIPD UIN Sunan Kalijaga harus menerapkan kontrol deteksi, pencegahan dan pemulihan untuk melindungi fasilitas terhadap malware kemudian dikombinasikan dengan kesadaran pengguna, PTIPD UIN Sunan Kalijaga juga harus membuat, menjaga dan meninjau secara berkala log peristiwa yang merekam aktivitas pengguna, pengecualian, kesalahan dan kejadian keamanan informasi, instansi PTIPD UIN Sunan Kalijaga pun harus mensinkronkan jam semua sistem pemrosesan informasi yang relevan dalam suatu organisasi atau domain keamanan ke sumber waktu dari satu referensi yang sama, dalam proses pengembangan persyaratan terkait dengan keamanan informasi harus dimasukkan dalam persyaratan untuk sistem informasi baru atau penyempurnaan terhadap sistem informasi yang sudah ada, serta PTIPD UIN Sunan Kalijaga harus menetapkan dan secara tepat melindungi pengembangan berkelanjutan yang aman untuk pengembangan sistem dan upaya integrasi yang mencakup seluruh *life cycle* dari pengembangan sistem, dan kemudian PTIPD harus meninjau sistem informasi secara berkala untuk kepatuhan terhadap kebijakan dan standar keamanan informasi yang berkaitan dengan pengamanan pihak eksternal, layanan infrastruktur awan (cloud) dan perlindungan data probadi pengguna.

DAFTAR PUSTAKA

Badan Siber dan Sandi Negara (2022) Konsultasi dan Assessment Indeks KAMI, BSSN. Available at: https://bssn.go.id/indeks-kami/ (Accessed: 7 November 2022).

BOGDAN, R.C.& B.K.S. (1998) Qualitative Research for Education: An Introduction to Theory and Methods. Edited by I. Allyn and Bacon. Boston London.

Chistensson, P. (2017) Elearning, techterms.com.

Gemalto (2017) Poor Internal Security Practices Take a Toll. Belcamp: Gemalto.

Harliana, P., Perdana, A. and Prasetyo, R.M. (2015) Sniffing dan Spoofing Pada Aspek Keamanan Komputer. Available at: https://www.academia.edu/5088063/Jurnal Keamanan-Komputer (Accessed: 11 November 2022).

Huizhi, C. (2022) Held for selling information on students, Shine.

Hutahaean, J. (2015) Konsep sistem informasi. Deepublish.

ID-Cert (2017) Laporan Akhir Tahun 2017. Jakarta.

Ponemon Institute LLC (2017) 2017 Cost of Data Breach Study. Michigan.

PTIPD UIN Sunan Kalijaga (2022) Sekilas PTIPD, PTIPD UIN Sunan Kalijaga Yogyakarta.

Tim Direktorat Keamanan Informasi (2011) Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik. Jakarta.

Whitman, M.E. and Mattord, H.J. (2021) Principles of information security. Cengage learning.