PERGURUAN TINGGI MUHAMMADIYAH
UNIVERSITAS AHMAD DAHLAN
LEMBAGA PENELITIAN DAN PENGABDIAN KEPADA MASYARAKAT
UAD Kampus 2 Unit B, Jl. Pramuka No. 5F, Pandeyan, Umbulharjo, Yogyakarta 55161, email : lppm@uad.ac.id

SURAT PERJANJIAN PELAKSANAAN PENELITIAN
Nomor : PUPS-278/SP3/LPPM-UAD/VI/2021

Pada hari ini, Selasa tanggal Satu bulan Juni tahun Dua ribu dua puluh satu (01-06-2021), kami yang bertandatangan di bawah ini :

1. Nama : Anton Yudhana, S.T., M.T., Ph.D.
   Jabatan : Kepala Lembaga Penelitian dan Pengabdian Kepada Masyarakat Universitas Ahmad Dahlan (LPPM UAD), selanjutnya disebut sebagai PIHAK PERTAMA.
2. Nama : Tawar Ag, S.Si., M.Kom.
   Jabatan : Dosen/Peneliti pada Program Studi Sistem Informasi Fakultas Sains dan Teknologi Terapan (FAST) Universitas Ahmad Dahlan (UAD), selaku Ketua Peneliti, selanjutnya disebut PIHAK KEDUA.

Kedua belah pihak menyatakan setuju dan mufakat untuk mengadakan perjanjian pelaksanaan penelitian untuk selanjutnya disebut Surat Perjanjian Pelaksanaan Penelitian (SP3) dengan ketentuan dan syarat-syarat sebagai berikut.

Pasal 1
DASAR HUKUM

(1) Hasil review/penilaian proposal yang dilakukan oleh Tim Reviewer Penelitian Internal UAD.
(2) Surat Keputusan Kepala LPPM UAD Nomor: U12.3/316/V/2021 tanggal 29 Mei 2021 tentang Penetapan Hasil Seleksi Proposal Penelitian Dana UAD Tahun Akademik 2020/2021.

Pasal 2
RUANG LINGKUP DAN JANGKA WAKTU PENELITIAN

(1) PIHAK PERTAMA memberikan pekerjaan kepada PIHAK KEDUA dan PIHAK KEDUA menyatakan menerima pekerjaan dari PIHAK PERTAMA berupa kegiatan penelitian sebagai berikut :

Skema	:	Penelitian Unggulan Program Studi
Judul penelitian	:	ASESMEN PENILAIAN KEAMANAN INFORMASI LAYANAN ZAKAT MENGGUNAKAN INDEKS KAMI 4.1
Jenis Riset	:	Terapan, TKT : 4
Luaran Wajib	:	Draft Naskah Kebijakan, Artikel di jurnal Internasional, Artikel di Jurnal Nasional Terakreditasi

(2) Jangka waktu pelaksanaan penelitian tersebut pada ayat (1) dimulai sejak ditandatangani SP3 ini sampai dengan batas akhir unggah Laporan Akhir Penelitian pada tanggal 31 Desember 2021

Pasal 3

PERSONALIA PELAKSANA PENELITIAN

Personalia pelaksana penelitian ini terdiri dari :

Ketua Peneliti	:	Tawar Ag, S.Si., M.Kom.
Pembimbing	:	-
Anggota	:	1. Dr. Imam Riadi, M.Kom

Pasal 4

BIAYA PENELITIAN DAN CARA PEMBAYARAN

(1) PIHAK PERTAMA menyediakan dana pelaksanaan penelitian kepada PIHAK KEDUA sejumlah Rp. 18.000.000,00 (Delapan Belas Juta Rupiah) yang dibebankan pada Anggaran Pendapatan dan Belanja (APB) LPPM UAD Tahun Akademik 2020/2021 dibayarkan melalui rekening bank atas nama Ketua Peneliti oleh Biro Keuangan dan Anggaran UAD sebagai berikut :

Nama	:	Tawar Ag, S.Si., M.Kom.
Nama Bank	:	BPD DIY SYARIAH
Nomor Rekening	:	801211007618

(2) Tahap I sebesar 70% x Rp 18.000.000,00 = Rp 12.600.000,00 (dua belas juta enam ratus ribu Rupiah), dibayarkan setelah SP3 ini ditandatangani oleh PARA PIHAK dan PIHAK KEDUA telah mengunggah file kontrak SP3 ini pada portal Penelitian UAD.

(3) Tahap II sebesar 30% x Rp 18.000.000,00 = Rp 5.400.000,00 (lima juta empat ratus ribu Rupiah), dibayarkan setelah (a) PIHAK KEDUA mengunggah Laporan Akhir Penelitian dan (b) luaran wajib penelitian dinyatakan tercapai.

(4) Jika sampai pada batas akhir penelitian PIHAK KEDUA hanya dapat mengunggah Laporan Akhir Penelitian dan TIDAK DAPAT merealisasikan luaran wajib, maka dana penelitian Tahap II hanya dapat dicairkan sebesar 15%.

Pasal 5

PELAKSANAAN PEMBIMBINGAN

(1) Khusus skema Penelitian Dosen Pemula (PDP), peneliti wajib melakukan pembimbingan atau konsultasi dengan dosen pembimbing penelitian paling sedikit 4 (empat) kali pembimbingan.

(2) Pembimbingan sebagaimana dimaksud dalam ayat (1) antara lain dalam hal-hal berikut.
a. penyusunan angket/kuesioner dan atau teknik pengumpulan data lainnya;
b. analisis data dan interpretasinya;
c. penyusunan hasil penelitian, pembahasan, penarikan kesimpulan;
d. penyusunan luaran penelitian.

(3) Pembimbingan sebagaimana dimaksud dalam ayat (1) dan ayat (2) dituliskan sesuai dengan template form pembimbingan yang tersedia.

Pasal 6

JENIS LAPORAN PENELITIAN

(1) PIHAK KEDUA wajib menyusun dan mengungah laporan penelitian melalui portal Penelitian UAD yang terdiri atas :
   a. Laporan Kemajuan
   b. Laporan Akhir
(2) Berkas Laporan Kemajuan digunakan sebagai bahan monitoring dan evaluasi (monev) internal, diunggah selambat-lambatnya tanggal 15 Oktober 2021.
(3) Berkas Laporan Akhir digunakan sebagai acuan pencairan dana Tahap II dan bahan pertimbangan berlanjut atau tidaknya kontrak penelitian tahun jamak (multi years), diunggah selambat-lambatnya tanggal 31 Desember 2021.

Pasal 7

LUARAN WAJIB PENELITIAN

(1) PIHAK PERTAMA berkewajiban untuk merealiasikan luaran wajib penelitian sebagaimana yang dijanjikan dalam proposal.
(2) Status minimal luaran wajib yang harus dicapai oleh PIHAK KEDUA adalah sebagai berikut. (i) accepted untuk jenis luaran artikel jurnal/seminar/konferensi, atau (ii) naik cetak untuk jenis luaran buku, atau (iii) diterima atau dibahas instansi pengguna untuk jenis luaran naskah akademik, atau (iv) telah terdaftar atau didaftarkan untuk jenis kekayaan intelektual (KI), atau (v) telah terwujud atau telah dilakukan uji laboratorium untuk jenis luaran purwarupa (prototipe), dan sejenisnya.

Pasal 8

MONITORING DAN EVALUASI

(1) PIHAK PERTAMA berhak untuk melakukan monitoring dan evaluasi (monev) pelaksanaan penelitian, baik secara administrasi maupun substansi.
(2) Pemantauan kemajuan penelitian dilakukan oleh Tim Monev yang dibentuk oleh PIHAK PERTAMA.
(3) Monev internal dilakukan terhadap dokumen Laporan Kemajuan yang diunggah oleh PIHAK KEDUA.
(4) PIHAK PERTAMA berhak untuk menentukan lanjut atau putusnya kontrak penelitian tahun jamak (multi years) berdasarkan hasil dari monev tahap II terhadap Laporan Akhir dan capaian luaran penelitian tahun berjalan yang diunggah PIHAK KEDUA.

Pasal 9

TANGGUNGAN PENELITIAN DAN LUARAN PENELITIAN

(1) Peneliti dinyatakan memiliki tanggungan penelitian apabila sampai pada masa penerimaan proposal penelitian periode berikutnya belum menyelesaikan kewajiban unggah Laporan Akhir Penelitian.
(2) Peneliti yang memiliki tanggungan penelitian sebagaimana dimaksud pada ayat (1) tidak diperkenankan mengajukan proposal penelitian pada periode tersebut.
(3) Peneliti dinyatakan memiliki tanggungan luaran penelitian apabila sampai pada masa akhir unggah Laporan Akhir Penelitian, luaran wajib belum tercapai dengan status minimal seperti disebutkan pada Pasal 7 ayat (2).

(4) Peneliti yang memiliki tanggungan luaran penelitian sebagaimana dimaksud pada ayat (3) masih diperkenankan mengajukan proposal penelitian pada periode terdekat.

(5) Peneliti yang belum memenuhi luaran wajib sampai pada penerimaan proposal penelitian pada periode tahun berkutnya tidak diperkenankan mengajukan proposal pada periode tersebut.

(6) Tanggungan penelitian dan/atau luaran wajib penelitian berlaku bagi Ketua dan Anggota peneliti dari Universitas Ahmad Dahlan.

Pasal 10
SANKSI DAN PEMUTUSAN PERJANJIAN PENELITIAN

(1) PIHAK PERTAMA berhak memberikan peringatan dan atau teguran atas kelalaian dan atau pelanggaran yang dilakukan oleh PIHAK KEDUA yang mengakibatkan tidak dapat terpenuhinya kontrak penelitian ini.

(2) PIHAK PERTAMA berhak melakukan pemutusan perjanjian penelitian, jika PIHAK KEDUA tidak mengindahkan peringatan yang diberikan oleh PIHAK PERTAMA.

(3) Segala kerugian material maupun finansial yang disebabkan akibat kelalaian PIHAK KEDUA, maka sepenuhnya menjadi tanggungjawab PIHAK KEDUA.

(4) Jenis sanksi yang diberikan dapat berupa :
(a) tidak diperkenankannya mengajukan proposal penelitian sebagaimana dimaksud pada Pasal 9 ayat (5) sampai kewajibannya terselesaikan; dan atau
(b) tidak dapat mencairkan dana Tahap II; dan atau
(c) mengembalikan dana yang telah diterima oleh PIHAK KEDUA.

Pasal 11
KEADAAN MEMAKSA (FORCE MAJEUR)

Ketentuan dalam Pasal 10 tersebut di atas tidak berlaku dalam keadaan sebagai berikut :

a. Keadaan memaksa (force majeur)
b. PIHAK PERTAMA menyetujui atas terjadinya keterlambatan yang didasarkan pada pemberitahuan sebelumnya oleh PIHAK KEDUA kepada PIHAK PERTAMA dengan Surat Pemberitahuan mengenai kemungkinan terjadinya keterlambatan dalam penyelesaian kegiatan penelitian sebagaimana dimaksud dalam Pasal 2; dan sebaliknya PIHAK KEDUA menyetujui terjadinya keterlambatan pembayaran sebagai akibat keterlambatan dalam penyelesaian perjanjian penelitian.

Pasal 12

(1) Keadaan memaksa (force majeur) sebagaimana yang dimaksud dalam Pasal 11 ayat (1) adalah peristiwa-peristiwa yang secara langsung mempengaruhi pelaksanaan perjanjian serta terjadi di luar kekuasaan dan kemampuan PIHAK KEDUA ataupun PIHAK PERTAMA.

(2) Peristiwa yang tergolong dalam keadaan memaksa (force majeur) antara lain berupa bencana alam, pemogokan, wabah penyakit, huru-hara, pemberontakan, perang, waktu kerja diperpendek oleh pemerintah, kebakaran dan atau peraturan pemerintah mengenai keadaan bahaya serta hal-hal lainnya yang dipersamakan dengan itu, sehingga PIHAK KEDUA ataupun PIHAK PERTAMA terpaksa tidak dapat memenuhi kewajibannya.

(3) Peristiwa sebagaimana dimaksud pada ayat (2) tersebut di atas, wajib dibenarkan oleh penguasa setempat dan diberitahukan dengan surat pemberitahuan oleh PIHAK KEDUA kepada PIHAK PERTAMA atau PIHAK PERTAMA kepada PIHAK KEDUA yang menyebutkan telah terjadinya peristiwa yang dikategorikan sebagai keadaan memaksa (force majeur).

(4) PIHAK PERTAMA memberikan kesempatan kepada PIHAK KEDUA untuk menyelesaikan perjanjian kontrak ini sampai pada batas waktu yang disepakati oleh PARA PIHAK jika keadaan force majeur dinyatakan telah selesai.

Pasal 13
PENYELESAIAN PERSELISIHAN

(1) Apabila dalam pelaksanaan perjanjian dan segala akibatnya timbul perbedaan pendapat atau perselisihan, PIHAK PERTAMA dan PIHAK KEDUA setuju untuk menyelesaikannya secara musyawarah untuk mencapai mufakat.

(2) Apabila penyelesaian sebagaimana termaksud dalam ayat (1) di atas tidak tercapai, maka PIHAK PERTAMA dan PIHAK KEDUA sepakat menyerahkan perselisihan tersebut melalui mediasi dengan Rektor sebagai atasan langsung dari PIHAK PERTAMA yang putusannya bersifat final dan mengikat.

Pasal 14
PENGUNDURAN DIRI

(1) Apabila PIHAK KEDUA mengundurkan diri atau membatalkan SP3 ini, maka PIHAK KEDUA wajib mengajukan Surat Pengunduran Diri yang ditujukan kepada PIHAK PERTAMA.

(2) Surat Pengunduran Diri sebagaimana dimaksud pada ayat (1) wajib disahkan oleh dekan fakultas ketua peneliti yang bersangkutan.

(3) PIHAK KEDUA wajib mengembalikan dana yang telah diterima kepada PIHAK PERTAMA

Pasal 15
LAIN-LAIN

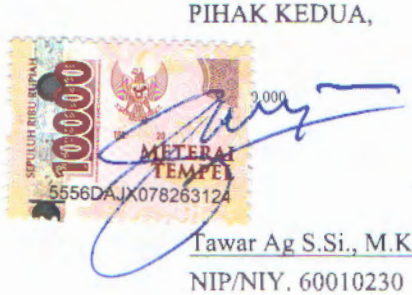
(1) Hal-hal yang dianggap belum cukup dan perubahan-perubahan perjanjian akan diatur kemudian atas dasar permufakatan kedua belah pihak yang akan dituangkan dalam bentuk Surat atau Perjanjian Tambahan (addendum), yang merupakan satu kesatuan dan bagian yang tidak terpisahkan dari perjanjian awal.

(2) Surat Perjanjian Pelaksanaan Penelitian (SP3) ini berlaku sejak ditandatangani dan disetujui oleh PARA PIHAK.

PIHAK PERTAMA,

Anton Yudhana, S.T., M.T., Ph.D.
NIP/NIY. 60010383

PIHAK KEDUA,



Tawar Ag S.Si., M.Kom.
NIP/NIY. 60010230

(3) Peristiwa sebagaimana dimaksud pada ayat (2) tersebut di atas, wajib dibenarkan oleh penguasa setempat dan diberitahukan dengan surat pemberitahuan oleh PIHAK KEDUA kepada PIHAK PERTAMA atau PIHAK PERTAMA kepada PIHAK KEDUA yang menyebutkan telah terjadinya peristiwa yang dikategorikan sebagai keadaan memaksa (force majeur).

(4) PIHAK PERTAMA memberikan kesempatan kepada PIHAK KEDUA untuk menyelesaikan perjanjian kontrak ini sampai pada batas waktu yang disepakati oleh PARA PIHAK jika keadaan force majeur dinyatakan telah selesai.

Pasal 13
PENYELESAIAN PERSELISIHAN

(1) Apabila dalam pelaksanaan perjanjian dan segala akibatnya timbul perbedaan pendapat atau perselisihan, PIHAK PERTAMA dan PIHAK KEDUA setuju untuk menyelesaikannya secara musyawarah untuk mencapai mufakat.

(2) Apabila penyelesaian sebagaimana termaksud dalam ayat (1) di atas tidak tercapai, maka PIHAK PERTAMA dan PIHAK KEDUA sepakat menyerahkan perselisihan tersebut melalui mediasi dengan Rektor sebagai atasan langsung dari PIHAK PERTAMA yang putusannya bersifat final dan mengikat.

Pasal 14
PENGUNDURAN DIRI

(1) Apabila PIHAK KEDUA mengundurkan diri atau membatalkan SP3 ini, maka PIHAK KEDUA wajib mengajukan Surat Pengunduran Diri yang ditujukan kepada PIHAK PERTAMA.

(2) Surat Pengunduran Diri sebagaimana dimaksud pada ayat (1) wajib disahkan oleh dekan fakultas ketua peneliti yang bersangkutan.

(3) PIHAK KEDUA wajib mengembalikan dana yang telah diterima kepada PIHAK PERTAMA

Pasal 15
LAIN-LAIN

(1) Hal-hal yang dianggap belum cukup dan perubahan-perubahan perjanjian akan diatur kemudian atas dasar permufakatan kedua belah pihak yang akan dituangkan dalam bentuk Surat atau Perjanjian Tambahan (addendum), yang merupakan satu kesatuan dan bagian yang tidak terpisahkan dari perjanjian awal.

(2) Surat Perjanjian Pelaksanaan Penelitian (SP3) ini berlaku sejak ditandatangani dan disetujui oleh PARA PIHAK.

PIHAK PERTAMA,	PIHAK KEDUA,
	Materai 10.000
Anton Yudhana, S.T., M.T., Ph.D.	Tawar Ag S.Si., M.Kom.
NIP/NIY. 60010383	NIP/NIY. 60010230

LAPORAN AKHIR PENELITIAN
SKEMA PENELITIAN UNGGULAN PROGRAM STUDI (PUPS)

ASESMEN PENILAIAN KEAMANAN INFORMASI LAYANAN ZAKAT MENGGUNAKAN INDEKS KAMI 4.1

TIM PENGUSUL:

Ketua : Tawar, S.Si., M.Kom.
Anggota : Dr. Imam Riadi, M.Kom

Anggota Mahasiswa : 1. Ariqah Adliana Siregar (1800016036)
2. Adiniah Gustika Pratiwi (1800016038)

PROGRAM STUDI SISTEM INFORMASI
FAKULTAS SAINS DAN TEKNOLOGI TERAPAN
UNIVERSITAS AHMAD DAHLAN
JANUARI 2022

HALAMAN PENGESAHAN
LAPORAN AKHIR PENELITIAN DANA INTERNAL UAD
TAHUN AKADEMIK 2021/2022

Judul Penelitian	:	ASESMEN PENILAIAN KEAMANAN INFORMASI LAYANAN ZAKAT MENGGUNAKAN INDEKS KAMI 4.1
Butir Renstra Prodi/Pusat	:	Program Studi
TSE Penelitian	:	20.05-Information, computer and communication
Jenis Riset	:	Terapan
Skala TKT	:	4

Ketua Peneliti

a. Nama Lengkap dan Gelar	:	TAWAR AG S.Si., M.Kom.
b. NIY/NIP	:	60010230
c. Fakultas/Program Studi	:	Sains dan Teknologi Terapan / Sistem Informasi
d. Pendidikan Terakhir	:	S2
e. Jabatan Akademik	:	Lektor

Anggota Peneliti

Nama Lengkap dan Gelar	:	1. IMAM RIADI, Dr., M.Kom (Sistem Informasi)

Anggota Peneliti Eksternal

Nama Lengkap dan Gelar	:	

Jumlah mahasiswa terlibat	:	2 orang
Lama Penelitian	:	7 bulan
Biaya Total Penelitian	:	Rp. 18.000.000,00
- Dana Disetujui	:	Rp. 18.000.000,00
- Sumber Dana Lain	:	Rp. 0,00

Menyetujui,
Kepala LPPM Universitas Ahmad Dahlan,

Anton Yudhana, S.T., M.T., Ph.D.
NIP/NIY. 60010383

Yogyakarta, 07 Januari 2022
Ketua Pengusul,

TAWAR AG S.Si., M.Kom.
NIP/NIY. 60010230

LAPORAN AKHIR PENELITIAN

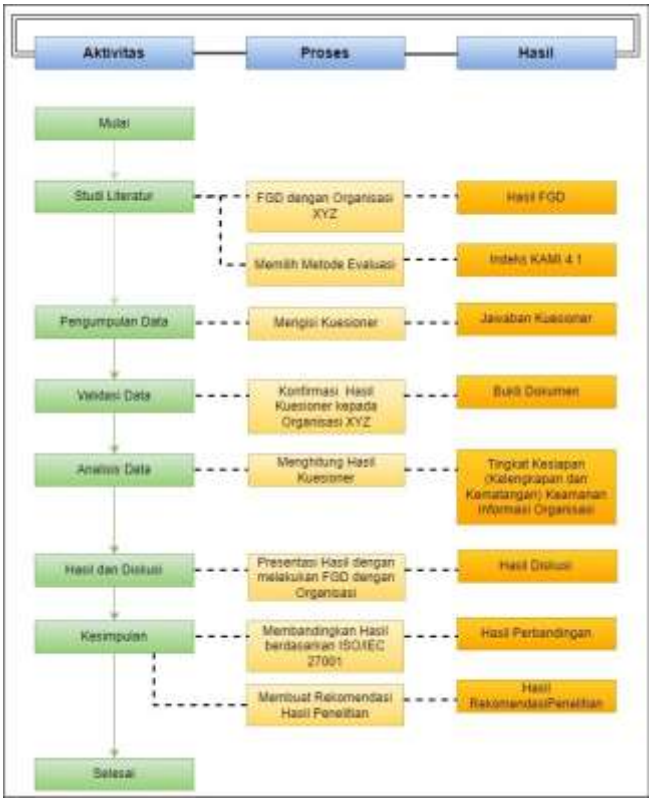
Ringkasan penelitian berisi: (i) latar belakang penelitian, (ii) tujuan penelitian, (iii) tahapan metode penelitian, (iv) luaran yang ditargetkan, (v) uraian TKT penelitian yang ditargetkan serta (vi) hasil penelitian yang diperoleh sesuai dengan tahun pelaksanaan penelitian.

RINGKASAN

Perkembangan teknologi informasi berkembang dengan pesat. Ancaman terhadap sumber daya informasi menuntut perlunya kebijakan manajemen keamanan informasi di setiap instansi. Indeks Keamanan Informasi (KAMI) adalah metode yang dikembangkan oleh Kementerian Komunikasi dan Informatika yang digunakan untuk mengevaluasi tingkat kematangan, kelengkapan penerapan ISO/IEC 27001:2013 dan kesiapan keamanan informasi. Lazismu sebagai lembaga zakat nasional telah memanfaatkan teknologi informasi pada beberapa sistem, diantaranya sistem *crowdfunding* dan sistem anggaran. Kedua sistem ini rentan terhadap akses illegal, namun secara internal di Lazismu belum pernah dilakukan pemeriksaan terhadap manajemen keamanan informasinya.

Penelitian ini bertujuan untuk melakukan penilaian dan memberikan rekomendasi bagi layanan *crowdfunding* dan sistem anggaran supaya berjalan dengan aman dan lancar menggunakan Index KAMI 4.1. Penelitian ini terdiri dari beberapa langkah, dimulai dengan melakukan observasi yang dilakukan pada Lazismu, proses berikutnya melalui kegiatan *focus group discussion* untuk menilai tingkat keamanan informasi layanan *crowdfunding* dan sistem anggaran.

Alur dan metode penelitian disajikan dalam gambar 1.



Gambar 1. Metodologi Penelitian

Analisis hasil perhitungan dijadikan dasar untuk pengembangan rekomendasi. Berdasarkan hasil penilaian yang dilakukan, layanan croudfunding memperoleh hasil nilai I sampai dengan I+, sementara pada sistem anggaran levelnya I+ s/d II. hal ini menunjukkan bahwa kedua sistem di Lazismu masih dalam kondisi awal belum menerapkan standar keamanan informasi dalam. Dalam hal kesiapan untuk sertifikasi ISO 27001, kedua sistem ini dapat dikatakan "Belum Memenuhi Syarat". Rekomendasi yang diusulkan untuk meningkatkan nilai dilakukan dengan cara menyusun dan menerapkan keamanan informasi dengan mengacu kontrol-kontrol yang ada pada ISO 27001.

Luaran dari peneltian ini terdiri dari dua artikel publikasi di journal JUITA dan IJACSA (LoSubmitted terlampir)

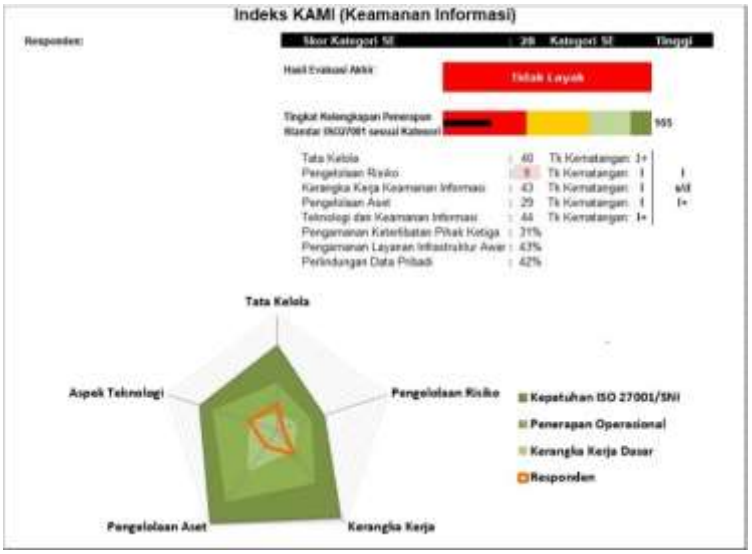
Kata kunci maksimal 5 kata kunci. Gunakan tanda baca titik koma (;) sebagai pemisah dan ditulis sesuai urutan abjad.

Kata Kunci : **Asesmen, Keamanan, Informasi, Indeks KAMI , Lazismu**

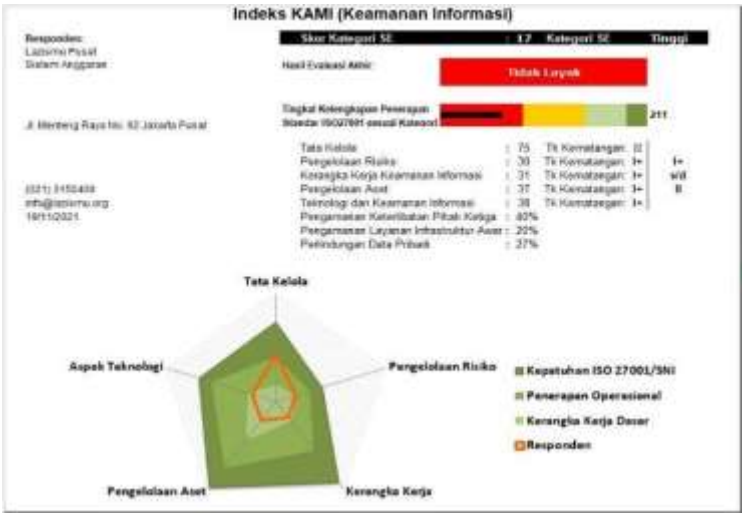
Hasil pelaksanaan penelitian berisi: (i) kemajuan pelaksanaan penelitian yang telah dicapai sesuai tahun pelaksanaan penelitian, (ii) data yang diperoleh, (iii) hasil analisis data yang telah dilakukan, (iv) pembahasan hasil penelitian, serta (v) luaran yang telah didapatkan. Seluruh hasil atau capaian yang dilaporkan harus berkaitan dengan tahapan pelaksanaan penelitian sebagaimana direncanakan pada proposal. **Penyajian data** dan **hasil penelitian** dapat berupa gambar, tabel, grafik, dan sejenisnya, serta **pembahasan hasil penelitian** didukung dengan sumber pustaka primer yang relevan dan terkini.

HASIL PELAKSANAAN PENELITIAN

Penelitian tingkat kematangan keamanan informasi pada sistem *crowdfunding disajikan berupa diagram radar pada gambar 2 dan gambar 3.*



Gambar 2. Dashboard hasil evaluasi sistem *crowdfunding*



Gambar 3. Dashboard hasil evaluasi *sistem anggaran*

Gambar 2 dan gambar 3 menunjukkan bahwa pada saat ini Sistem Crowdfunding berada pada tingkat kematangan I hingga I+ , sementara Sistem Anggaran berada pada tingkat kematangan I+ hingga II. Ambang batas minimum kesiapan sertifikasi tingkat kematangan yang diharapkan adalah Tingkat III+, artinya kedua sistem yang ada di Lazismu saat ini berada dalam kondisi tingkat awal atau belum memenuhi syarat untuk diusulkan dalam sertfikasi ISO27001.

1. **Kategori Sistem Elektronik**
   Kategori Sistem Elektronik (SE) merupakan kategori pertama pada Indeks KAMI yang mengevaluasi tingkat sistem elektronik yang digunakan. Dalam Kategori SE terdapat tiga kategori hasil yaitu rendah, tinggi dan strategis. Kategori SE memiliki 10 pertanyaan dengan nilai maksimum 50. Hasil yang didapatkan pada kategori Sistem Elektronik berdasarkan penilaian Indeks KAMI didapatkan skor sebesar 28 untuk crowdfunding dan skor 17 untuk sistem anggaran, seperti disajikan pada tabel 2. Perolehan skorini berarti kedua sistem masuk ke dalam kategori TINGGI sesuai dengan tabel tingkat kematangan Indeks KAMI dimana kategori Tinggi berkisar antara skor 16 sampai dengan 34, sebagai panduan penilaian dapat dilihat pada tabel 1.

Tabel 1. Skor Kategori Sistem Elektronik Indeks KAMI

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

Tabel 2. Perolehan Skorkategori SE

Skoryang diperoleh		Kategori
Crowdfunding	28	Tinggi
Anggaran	17	Tinggi

2. **Kategori Tatakelola Keamanan Informasi**
   Kategori Tatakelola merupakan kategori kedua pada Indeks KAMI yang mengevaluasi tingkat tatakelola pada sistem yang digunakan. Penilaian Tata Kelola Keamanan Informasi menggunakan 22 pertanyaan dan mendapatkan total nilai evaluasi sebesar 40 untuk crowdfunding dengan status tingkat kematangan I+ dan nilai 75 untuk sistem anggaran dengan status tingkat kematangan II.

Berdasarkan tabel 3 Tatakelola keamanan informasi pada sistem crowdfunding yaitu sudah adanya pemahaman terkait keamanan infromasi yang cukup besar didalam instansi, mendokumentasikan setiap tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya dan belum mendefinisikan kebijakan langkah pidana terhadap insiden keamanan informasi. Sistem anggaran berada pada tingkat penerapan kerangka kerja dasar.

Tabel 3. Hasil evaluasi kategori Tatakelola

Status Pengamanan	Tingkat kematangan													
	Crowdfunding							Anggaran						
	1	SK	2	SK	3	SK	Total	1	SK	2	SK	3	SK	Total
Tidak dilakukan	0	0	0	0	0	2	0	0	0	0	0	0	0	0
Dalam perencanaan	1	2	2	3	3	3	8	1	0	2	0	3	0	0
Dalam penerapan atau di terapkan sebagian	2	5	4	4	6	1	26	2	10	4	20	6	18	48
Diterapkan menyeluruh	3	0	6	1	9	0	6	3	9	6	18	9	0	27
Total Skor							40	Total Skor						75
Tingkat kematangan							(I+)	Tingkat kematangan						II

*) SK : Skor

3. Kategori Pengelolaan Risiko Keamanan Informasi

Kategori Pengelolaan Risiko merupakan kategori ketiga pada Indeks KAMI yang mengevaluasi tingkat risiko pada sistem yang digunakan. Penilaian Resiko Keamanan Informasi *system crowdfunding* menggunakan 16 pertanyaan mendapatkan total nilai evaluasi Risiko Keamanan Informasi sebesar 9 dari dengan status tingkat kematangan I, sedang nilai pada sistem anggaran adalah 75.

Pengeloaan Risiko Keamanan Informasi pada *system crowdfunding* valid ditingkat kematangan I yang artinya dalam kondisi awal. Pada sistem ini sudah ada pemahaman mengenai perlunya pengelolaan keamanan informasi dan sangat perlu untuk ditingkatkan. Berdasarkan tabel 3 Risiko keamanan informasi pada sistem crowdfunding perlu mengidentifikasi ancaman dan kelemahan yang terkait dengan aset informasi, menyusun langkah mitigasi dan penanggulangan risiko, melakukan pemeriksaan mitigasi risiko secara berkala melakukan pengkajian secara berkala pada kerangka kerja pengelolaan risiko untuk memastikan / meningkatkan efektifitasnya. Sedang tingkat kematangan pada sistem keuangan adalah I+ .

Tabel 4. Hasil evaluasi kategori Risiko

Status Pengamanan	Tingkat kematangan													
	Crowdfunding							Anggaran						
	1	SK	2	SK	3	SK	Total	1	SK	2	SK	3	SK	Total
Tidak dilakukan	0	2	0	4	0	0	0	0	0	0	0	0	0	0
Dalam perencanaan	1	7	2	0	3	0	7	1	2	2	2	3	0	4
Dalam penerapan atau di terapkan sebagian	2	1	4	0	6	0	2	2	16	4	4	6	0	20
Diterapkan menyeluruh	3	0	6	0	9	0	0	3	0	6	6	9	0	6
Total Skor							9	Total Skor						30
Tingkat kematangan							I	Tingkat kematangan						I+

4. Kategori Kerangka Kerja Pengelolaan Keamanan Informasi

Kategori kerangka kerja merupakan kategori keempat pada Indeks KAMI yang mengevaluasi kerangka kerja pada sistem yang digunakan. Penilaian Kerangka Kerja Pengeloaan Informasi menggunakan 29 pertanyaan, pada *system crowdfunding* mendapatkan total nilai evaluasi sebesar 43 dengan status tingkat kematangan I. Sedangkan pada sistem anggaran diperoleh nilai 31 dengan status tingkat kematangan I+.

Area Kerangka Kerja Pengeloaan Informasi berada ditingkat kematangan I yang artinya dalam kondisi awal. Berdasarkan tabel 5 Kerangka Kerja keamanan informasi pada sistem crowdfunding perlu menentukan kebijakan pengembangan sistem yang aman, diperlukan pengendalian audit sistem informasi dan memverifikasi, meninjau, dan mengevaluasi kesinambungan keamanan informasi.

Tabel 5. Hasil evaluasi kategori Kerangka Kerja

Status Pengamanan	Tingkat kematangan													
	Crowdfunding							Anggaran						
	1	SK	2	SK	3	SK	Total	1	SK	2	SK	3	SK	Total
Tidak dilakukan	0	3	0	4	0	2	0	0	0	0	0	0	0	0
Dalam perencanaan	1	4	2	0	3	2	4	1	4	2	6	3	0	10
Dalam penerapan atau di terapkan sebagian	2	2	4	2	6	1	12	2	4	4	8	6	0	12
Diterapkan menyeluruh	3	1	6	4	9	2	27	3	9	6	0	9	0	9
Total Skor							43	Total Skor						31
Tingkat kematangan							I	Tingkat kematangan						I+

5. Kategori Pengelolaan Aset Informasi

Kategori Pengelolaan Aset merupakan kategori kelima pada Indeks KAMI yang mengevaluasi pengelolaan aset pada sistem yang digunakan. Penilaian Pengelolaan Aset Informasi menggunakan 38 pertanyaan, pada *system crowdfunding* didapatkan total nilai evaluasi sebesar 29 dengan status tingkat kematangan I. Sedangkan pada sistem anggaran diperoleh nilai 37 dengan status tingkat kematangan I+.

Pada area Pengelolaan Aset Informasi valid ditingkat kematangan I yang artinya dalam kondisi awal. Berdasarkan tabel 6 Pengelolaan Aset Keamanan Informasi pada sistem crowdfunding perlu melindungi segala asset (kantor, ruangan dan fasilitas) dari ancaman lingkungan akhir eksternal, memastikan prosedur Hak kekayaan intelektual dan pengamanan akses yang digunakan.

Tabel 6. Hasil evaluasi kategori Pengelolaan Aset

Status Pengamanan	Tingkat kematangan													
	Crowdfunding							Anggaran						
	1	SK	2	SK	3	SK	Total	1	SK	2	SK	3	SK	Total
Tidak dilakukan	0	13	0	7	0	3	0	0	0	0	0	0	0	0
Dalam perencanaan	1	3	2	1	3	1	5	1	6	2	2	3	0	8
Dalam penerapan atau di terapkan sebagian	2	8	4	2	6	0	24	2	14	4	12	6	0	26
Diterapkan menyeluruh	3	0	6	0	9	0	0	3	3	6	0	9	0	3
Total Skor							29	Total Skor						37
Tingkat kematangan							I	Tingkat kematangan						I+

6. Kategori Teknologi dan Keamanan Informasi

Kategori Teknologi Keamanan Informasi merupakan kategori keenam pada Indeks KAMI yang mengevaluasi teknologi pada sistem yang digunakan. Penilaian Pengelolaan Teknologi dan Keamanan Informasi menggunakan 26 pertanyaan, Pada *system crowdfunding* didapatkan total nilai evaluasi sebesar 44 dengan status tingkat kematangan I+. Sedangkan pada sistem anggaran diperoleh nilai 38 dengan status tingkat kematangan I+ juga.

Pada area Teknologi dan Keamanan Informasi valid ditingkat kematangan I+ yang artinya dalam kondisi awal. Berdasarkan tabel 7 Teknologi keamanan informasi pada sistem crowdfunding perlu membuat Kontrol terhadap malware dan jaringan.

Tabel 7. Hasil evaluasi kategori Teknologi dan Keamanan Informasi

Status Pengamanan	Tingkat kematangan													
	Crowdfunding							Anggaran						
	1	SK	2	SK	3	SK	Total	1	SK	2	SK	3	SK	Total
Tidak dilakukan	0	5	0	4	0	2	0	0	0	0	0	0	0	0
Dalam perencanaan	1	1	2	1	3	0	3	1	1	2	0	3	0	1
Dalam penerapan atau di terapkan sebagian	2	7	4	3	6	0	26	2	14	4	8	6	0	22
Diterapkan menyeluruh	3	1	6	2	9	0	15	3	3	6	12	9	0	15
Total Skor							44	Total Skor						38
Tingkat kematangan							I+	Tingkat kematangan						I+

7. Kategori Suplemen

Kategori Suplemen merupakan kategori ketujuh atau terakhir pada Indeks KAMI. Hasil evaluasi pada kategori ini disajikan pada tabel 8.

Tabel 8. *Hasil evaluasi kategori Suplemen*

Aspek	Tingkat kematangan	
	Crowdfunding	Anggaran
Pengamanan keterlibitan pihak ketiga	31%	40%
Pengamanan layanan infrastruktur awan	43%	20%
Perlindungan data pribadi	42%	27%

Skor yang didapat dari perhitungan kategori suplemen ini tidak mempengaruhi total skor dari bagian I sampai bagian VI dalam penilaian Indeks KAMI yang menunjukkan tingkat kesiapan dan kematangan pengamanan informasi. Berdasarkan Indeks KAMI penilaian kategori suplemen ini bertujuan untuk mendeteksi munculnya resiko keamanan informasi baru dengan adanya keterlibatan ketiga aspek tersebut.

Status luaran berisi **identitas** dan **status ketercapaian setiap luaran wajib** dan **luaran tambahan** (jika ada) yang dijanjikan. Jenis luaran dapat berupa publikasi, perolehan kekayaan intelektual, hasil pengujian atau luaran lainnya yang telah dijanjikan pada proposal. Uraian status luaran harus didukung dengan **bukti kemajuan** ketercapaian luaran sesuai dengan luaran yang dijanjikan. Lengkapi isian jenis luaran yang dijanjikan serta **lampirkan bukti dokumen** ketercapaian luaran wajib dan luaran tambahan.

STATUS LUARAN

Luaran Wajib

1. Draft Naskah Kebijakan : Buku Panduan Kebijakan Keamanan Informasi Berbasis Indeks KAMI (proses pengajuan Hak Cipta)
2. Artikel di journal internasional : IJACSA (terkirim, menunggu approval)
3. Artikel di jurnal nassional terakreditasi : JUITA (terkirim, menunggu approval)

Peran Mitra berupa **realisasi kerjasama** dan **kontribusi Mitra** baik *in-kind* maupun *in-cash* (untuk Penelitian Terapan dan Pengembangan). **Bukti pendukung** realisasi kerjasama dan realisasi kontribusi mitra **dilaporkan** sesuai dengan kondisi yang sebenarnya. **Lampirkan bukti dokumen** realisasi kerjasama dengan Mitra.

PERAN MITRA

- Pihak Lazismu memyambut baik dengan menyiapkan sejumlah personil sebagai nara sumber dalam penelitian ini.
- Hasil penelitian ini diterima dengan baik dan akan ditindaklanjuti untuk dijadikan salah satu topik pembahasan dalam Rapat Kerja Nasional (Rakernas) Lasismu Pusat yang rencananya akan diadakan antara tanggal 1 - 15 Januari 2022.
- Dalam forum Rakernas nanti, akan dibahas langkah-langkah sebagai tindak lanjut atas rekomendasi penelitian ini, yaitu pemenuhan terhadap ketentuan ISO 27001: 2013

Kendala Pelaksanaan Penelitian berisi **kesulitan** atau **hambatan** yang dihadapi selama melakukan penelitian dan mencapai luaran yang dijanjikan, termasuk **penjelasan jika** pelaksanaan penelitian dan luaran penelitian **tidak sesuai** dengan yang direncanakan atau dijanjikan.

KENDALA PELAKSANAAN PENELITIAN

- Situasi pandemi, semua pertemuan hanya bisa dilaksanakan secara virtual. Hal ini berdampak pada kelancaran komunikasi antara tim peneliti dan pihak Lazismu
- Situasi kelembagaan Lazismu yang belum ada unit kerja khusus untuk pengelolaan infrastruktur TIK, berakibat sedikit mengalami kesulitan saat awal menentukan personil yang sesuai.

Rencana Tindak Lanjut Penelitian berisi uraian rencana tindaklanjut penelitian selanjutnya dengan melihat hasil penelitian yang telah diperoleh. Jika ada target yang belum diselesaikan pada akhir tahun pelaksanaan penelitian, pada bagian ini dapat dituliskan rencana penyelesaian target yang belum tercapai tersebut.

RENCANA TINDAK LANJUT PENELITIAN

Sesuai rekomendasi Indeks KAMI, bahwa pengukuran dilakukan 2x dalam setahun, maka disarankan dilakukan pengukuran ulang semester berikutnya. Tim penelitian siap membantu melakukan pengukuran ulang.

Selanjutnya Lazismu disarankan :

- Untuk lebih menyiapkan diri dalam memenuhi kaidah-kaidah-kaidah yang ada pada kontrolnya ISO270001:2013.
- Melakukan Penetration Test (PenTest) terhadap aplikasi sistem anggaran dan sistem crowdfunding baik secara mandiri ataupun menggunakan tim professional.
- Perlu MOU sebagai payung kerjasama kelembagaan antara UAD dan Lazismu

Daftar Pustaka disusun dan ditulis **berdasarkan sistem nomor** sesuai dengan urutan pengutipan. **Hanya pustaka yang disitasi/diacu** pada laporan kemajuan saja yang dicantumkan dalam Daftar Pustaka.

DAFTAR PUSTAKA

[1] E. R. Pratama, Suprapto, dan A. R. Perdanakusuma, "Evaluation of Information Technology Security System Governance Using the KAMI Index and ISO 27001: A Case Study of KOMINFO East Java Province," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 11, hal. 5911–5920, 2018, [Daring]. Tersedia pada: http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/3465.

[2] T. Effendy *et al.*, "Evaluation of Information Security Using the Information Security Index (US) at the Regional Office of the Ministry of Law and Human Rights Diy," vol. 3, no. 1, hal. 1–6, 2020.

[3] B. Sutara, "PDAM Titra Medal Information Security Measurement Using the US Index for Information Security Maturity Level Analysis," vol. 17, no. 2, hal. 34–41, 2018, [Daring]. Tersedia pada: https://ejournal.ikmi.ac.id/index.php/jict-ikmi/article/view/32.

[4] Yustanti, W. Rahadian, B. Anita, Q. Prihanto, dan Agus, "Analysis Of Readiness And Maturity Level Of Implementation Of Iso 27001: 2013 Using Information Security Index 3: 2015 At Upt . Ppti State University Surabaya The Ministry of Communication and Information Technology of the Republic of Indonesia has issued regulation number," *Inform. P. T., Inform. J. T., Surabaya, U. N., Hari, D., Bulan, T., Hari, D., Bulan, T. (2016). Anal. Tingkat Kesiapan Dan Kematangan Implementasi Iso 27001 2013 Menggunakan Indeks Keamanan Inf. 3 2015 Pada Upt . Ppti Univ. N*, no. 4, hal. 1602–1613, 2016.

[5] M. R. Slamet, F. Wulandari, dan D. Amalia, "Assessment of Technology Security in Electronic Learning Systems Using the Information Security Index at Batam State Polytechnic," *J. Appl. Bus. Adm.*, vol. 3, no. 1, hal. 162–171, 2019, doi: 10.30871/jaba.v3i1.1305.

[6] W. W. W. S. Haries Anom Suseyto Aji Nugroho, "The syllogism method and for the validity of the answers from respondents in the analysis of the Maturity Level of Information Security Based on Sni Iso 27001:2013 at the Department of Population and Civil Registration of the City of Xyz," *J. Transform.*, vol. 14, no. 2, 2019.

[7] J. F. Andry dan A. K. Setiawan, "It Governance Evaluation Using Cobit 5 Framework on the National Library," *J. Sist. Inf.*, vol. 15, no. 1, hal. 10–17, 2019, doi: 10.21609/jsi.v15i1.790.

[8] Y. Sekhara, H. Medromi, dan H. Nahla, "Multi Agent Decision system for the IT Governance Platform," vol. 15, no. 5, hal. 290–306, 2017.

[9] A. R. Riswaya, A. Sasongko, dan A. Maulana, "Evaluation of Information Technology Security Governance Using Our Index for Preparation of Sni Iso/Iec 27001 Standard (Case Study: Stmik Mardira Indonesia)," *J. Comput. Bisnis, Vol. 14, No. 1, Juni 2020, 10-18 ISSN 1978-9629, ISSN 2442-4943*, vol. 14, no. 1, hal. 10–18, 2020.

[10] N. A. Widodo dan and A. F. R. , R. Rizal Isnanto, “Information Security Management System Planning And Implementation Based On Iso/Iec 27001:2005 StandardS (Case Study in a National Private Bank),” vol. 4, no. 1, hal. 60–66, 2016.

[11] N. E. Wowor *et al.*, “AAnalysis of Manado City Government Information Security Using Our Index,” *J. Tek. Inform.*, vol. 13, no. 3, hal. 1–10, 2018, doi: 10.35793/jti.13.3.2018.28081.

[12] T. Hartati, “Information Security Management System Planning in Academic Field Using ISO 27001: 2013,” *KOPERTIP J. Ilm. Manaj. Inform. dan Komput.*, vol. 1, no. 2, hal. 63–70, 2017, doi: 10.32485/kopertip.v1i02.24.

[13] F. Febrianto dan D. I. Sensuse, “Evaluation of information security using ISO / IEC 27002: a case study on the Banjarnegara Tunas Bangsa,” *Infokam*, vol. 2, no. 2013, hal. 21–27, 2017.

[14] R. C. Annisyah, A. Budiono, dan R. Fauzi, “Analysis And Design Of Information Security Management Directorate Of Information Systems Of Telkom University Using The Information Security Index (Kami) In The Area Of Information Asset Management, Technology And Information Security” vol. 8, no. 2, hal. 2663–2677, 2021.

[15] N. Matondang, I. N. Isnainiyah, dan A. Muliawatic, “Analysis of Information System Data Security Risk Management (Case Study: XYZ Hospital),” *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 2, no. 1, hal. 282–287, 2018, doi: 10.29207/resti.v2i1.96.

[16] W. Apriandari dan A. Sasongko, “Information Security Management System Analysis Using Sni Iso / Iec 27001: 2013 in the Regional Government of Sukabumi City (Case Study: At Diskominfo Sukabumi City),” *Ilm. SANTIKA*, vol. 8, no. 1, hal. 715–729, 2018.

[17] R. Adi, P. Pratama, R. Sengkey, dan C. Punusingon, “Information Security Analysis of Southeast Minahasa District Government Using KAMI Index,” vol. 15, no. 3, hal. 189–198, 2020.

[18] B. A. Firzah, “Evaluation of Information Security Management Using the Information Security Index (US) Based on Iso / Iec 27001: 2013 at the Directorate of Information Technology and System Development (Dptsi) Its Surabaya Evaluating Information Security Management Using KAMI Index,” vol. 6, no. 1, 2017.

[19] H. Hambali dan P. Musa, “Analysis of Governance Security Management Information System Using Index Kami in Central Government Institution,” *Angkasa J. Ilm. Bid. Teknol.*, vol. 12, no. 1, 2020, doi: 10.28989/angkasa.v12i1.563.

[20] M. Bakri dan N. Irmayana, “Analysis and Implementation of Simhp Bpkp Information Security Management System Using ISO 27001 Standard,” *J. Tekno Kompak*, vol. 11, no. 2, hal. 41, 2017, doi: 10.33365/jtk.v11i2.162.

[21] M. Lenawati, W. W. Winarno, dan A. Amborowati, “Information Security Governance in PDAM Using ISO/IEC 27001:2013 and COBIT 5,” *Sentra Penelit. Eng. dan Edukasi*, vol. 9, no. 1, hal. 44–49, 2017, [Daring]. Tersedia pada: http://speed.web.id/jurnal/index.php/speed/article/view/220.

[22] Y. C. Pradipta, Y. Rahardja, M. N. N. Sitokdana, U. Kristen, dan S. Wacana, “Information and Communication Technology of Aviation and Space (Pustikpan) Using Sni Iso / Iec 27001: 2013,” hal. 352–358, 2013.

[23] W. C. Pamungkas dan F. T. Saputra, “Evaluation of Information Security at SMA N 1 Sentolo Based on Information Security Index (KAMI) ISO/IEC 27001:2013,” *J. Sist. Komput. dan Inform.*, vol. 1, no. 2, hal. 101, 2020, doi: 10.30865/json.v1i2.1924.

[24] D. A. Wati, A. Budiono, dan R. Fauzsi, “Analysis And Design Of Information Security Management In The Directorate Of Telkom University Information Systems With Information Security Index (Us) In Security Governance Area Of Information, Risk

Management Of Information Security And Information Framework For Information Security Management," *Αγαη*, vol. 8, no. 5, hal. 55, 2019.

[25] BSSN, "Information Security Index (KAMI Index)," *Badan Siber dan Sandi Negara*, no. November, 2019.

Lampiran – lampiran :

1. Draft Naskah Kebijakan :
    a. Sertifikat HKI (dalam proses pendaftaran)
    b. Buku **"Panduan Kebijakan Keamanan Informasi Berbasis Indeks KAMI"**
2. Artikel di journal internasional :
    a. Bukti Terkirim ke Jurnal IJACSA
    b. Artikel terkirim ke IJACSA,
3. Artikel di jurnal nassional terakreditasi :
    a. Bukti Terkirim ke Jurnal JUITA
    b. Artikel terkirim ke JUITA

REPUBLIK INDONESIA
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA

SURAT PENCATATAN
CIPTAAN

Dalam rangka pelindungan ciptaan di bidang ilmu pengetahuan, seni dan sastra berdasarkan Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta, dengan ini menerangkan:

Nomor dan tanggal permohonan	:	EC00202201855, 8 Januari 2022
Pencipta		
Nama	:	**Tawar, Imam Riadi dkk**
Alamat	:	Sanggrahan UH 1/608, Semaki, Umbulharjo , Yogyakarta, DI YOGYAKARTA, 551166
Kewarganegaraan	:	Indonesia
Pemegang Hak Cipta		
Nama	:	**UNIVERSITAS AHMAD DAHLAN**
Alamat	:	Jl. Pramuka 5F, Pandeyan, Umbulharjo , Yogyakarta, DI YOGYAKARTA, 55161
Kewarganegaraan	:	Indonesia
Jenis Ciptaan	:	**Buku**
Judul Ciptaan	:	**Buku Panduan Kebijakan Keamanan Informasi Berbasis Indeks KAMI**
Tanggal dan tempat diumumkan untuk pertama kali di wilayah Indonesia atau di luar wilayah Indonesia	:	7 Januari 2022, di Yogyakarta
Jangka waktu pelindungan	:	Berlaku selama hidup Pencipta dan terus berlangsung selama 70 (tujuh puluh) tahun setelah Pencipta meninggal dunia, terhitung mulai tanggal 1 Januari tahun berikutnya.
Nomor pencatatan	:	000317065

adalah benar berdasarkan keterangan yang diberikan oleh Pemohon.
Surat Pencatatan Hak Cipta atau produk Hak terkait ini sesuai dengan Pasal 72 Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta.

a.n Menteri Hukum dan Hak Asasi Manusia
Direktur Jenderal Kekayaan Intelektual
u.b.
Direktur Hak Cipta dan Desain Industri

Dr. Syarifuddin, S.T., M.H.
NIP.197112182002121001

LAMPIRAN PENCIPTA

No	Nama	Alamat
1	Tawar	Sanggrahan UH 1/608, Semaki, Umbulharjo
2	Imam Riadi	Gamping Lor, Ambarketawang, Gamping
3	Adiniah Gustika Pratiwi	Tunggal Warga, Banjar Agung
4	Ariqah Adlianan Siregar	Seresam, Seberida

Buku Panduan

KEBIJAKAN KEMANAN INFORMASI BERBASIS INDEKS KAMI

Oleh :

Tawar, Imam Riadi,
Adiniah Gustika Pratiwi,
Ariqah Adliana Siregar

KATA PENGANTAR

Puji syukur ke hadirat Allah Swt, atas seluruh hidayah-Nya, penulisan buku panduan penilaian keamanan informasi Berbasis Indeks KAMI selesai dilakukan. Buku ini merupakan salah satu luaran dari penelitian yang berjudul "**Asesmen Penilaian Keamanan Informasi Layanan Zakat Menggunakan Indeks Kami 4.1"** dari Program Studi Sistem Informasi Universitas Ahmad Dahlan.

Penelitian ini dilakukan melalui pendanaan dari Lembaga Penelitian dan Pengabdian kepada Masyarakat Universitas Ahmad Dahlan (LPPM UAD) dengan skema Penelitian Unggulan Program Studi tahun 2021.

Luaran penelitian ini semoga dapat dimanfaatkan oleh pihak-pihak yang membutuhkan, khususnya adalah para pengelola sistem informasi, agar lebih tanggap terhadap tata kelola keamanan data dan informasi yang dimiliki.

Ungkapan terimakasih kami sampaikan kepada Lazismu, LPPM UAD, Program studi Sistem Informasi, seluruh anggota penelitian dan pihak-pihak terkait yang telah mendukung berjalannya penelitian ini dengan baik.

Seluruh tim menyadari naskah hasil penelitian ini jauh dari sempurna, untuk itu kami mengharapkan adanya saran dan kritik yang membangun untuk perbaikan.

Yogyakarata, 5 Januari 2022

Tim Peneliti:

Tawar, S.Si, M.Kom

Dr. Imam Riadi, M.Kom

Adiniah Gustika Pratiwi

Ariqah Adliana Siregar

DAFTAR ISI

SEKILAS TENTANG KEBIJAKAN INDEKS KEAMANAN INFORMASI

Indeks KAMI merupakan suatu alat evaluasi untuk menganalisa tingkat kesiapan pengamanan informasi di suatu organisasi. Alat ini tidak ditujukan untuk mengnalisakelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi/Perusahaan. Evaluasi ini dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan pembahasan yang memenuhi aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2013 (Nugroho, 2019).

Bentuk evaluasi yang diterapkan dalam indeks KAMI dirancang agar dapat digunakan oleh suatu organisasi dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan TIK dalam mendukung terlaksananya proses yang ada. Data yang digunakan dalam evaluasi ini nantinya akan memberikan gambaran indeks kesiapan - dari aspek kelengkapan maupun kematangan - kerangka kerja keamanan informasi yang diterapkan dan dapat digunakan sebagai pembanding dalam rangka menyusun langkah perbaikan dan penetapan prioritasnya (BSSN, 2019).

TUJUAN DAN MANFAAT PENILAIAN INDEKS KEAMANAN INFORMASI

TUJUAN

Tujuan dari penilaian Indeks Keamanan Informasi ini adalah sebagai berikut:

1. Untuk mengetahui tingkat kesiapan keamanan informasi pada suatu Instansi/Perusahaan.
2. Untuk mengetahui gambaran mengenai kematangan program kerja keamanan informasi yang dijalankan

Penilaian Indeks Keamanan Informasi ini dilakukan sebagai upaya pengamanan data dan aset informasi dari ancaman untuk keberlangsungan suatu bisnis dalam Instansi/Perusahaan, meminimalisir dampak yang ditimbulkan dari ancaman tersebut.

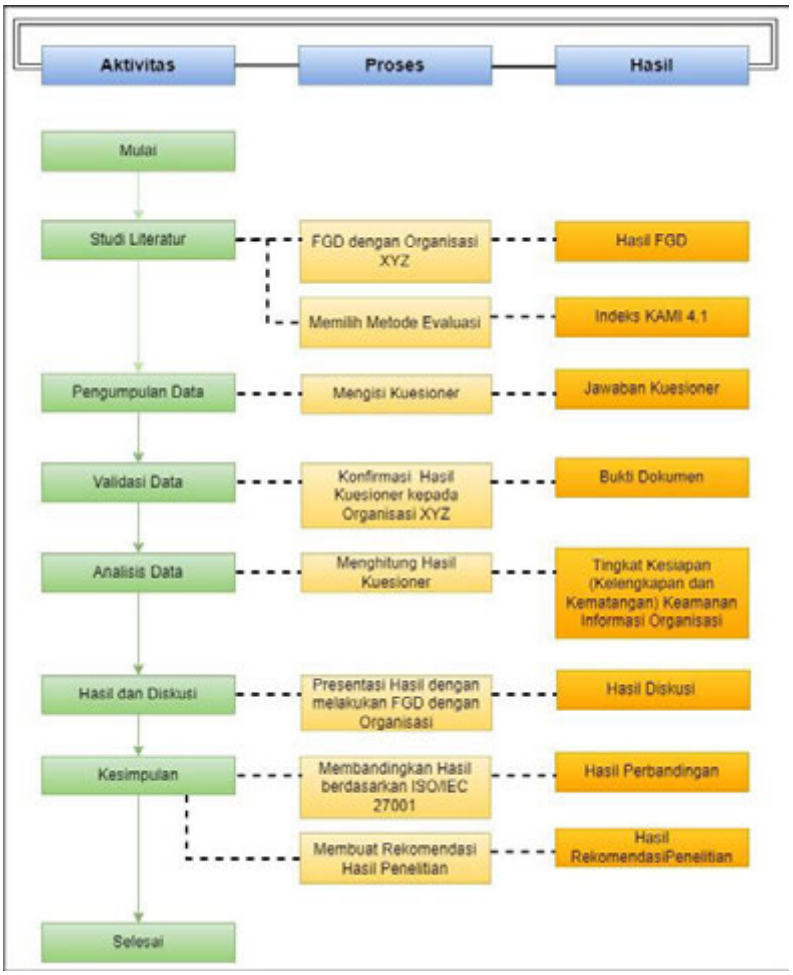
TUJUAN DAN MANFAAT PENILAIAN INDEKS KEAMANAN INFORMASI

MANFAAT

1. Membantu Instansi/Perusahaan mengetahui kondisi terkait dengan sistem manajemen keamanan informasi.
2. Memberikan masukan kepada Instansi/Perusahaan dalam meningkatkan kesiapan keamanan informasi pada sistem anggaran di Lazismu.

PETUNJUK PENILAIAN INDEKS KEAMANAN INFORMASI

Di bawah ini adalah gambaran alur secara keseluruhan dalam penilaian Indeks Keamanan Informasi.



Adapun detail alur penilaian dijelaskan sebagai berikut:

1. Studi Literatur

   FGD bersama dengan Instansi/Perusahaan merupakan proses awal dalam studi literatur. FGD dilakukan guna mengetahui permasalahan mengenai sistem yang ada dan mengetahui sistem apa saja yang akan digunakan dalam penelitian ini.

   Setelah mendapatkan hasil dari FGD maka selanjutnya adalah menetukan atau memilih metode apa yang dapat menyelesaikan permasalahan yang ada di Instansi/Perusahaan. Studi literatur dilakukan dengan meninjau penelitian sebelumnya yang mana

relevan dengan penelitian yang akan dilakukan kemudian memilih metode Indeks KAMI 4.1 sesuai dengan standar ISO/IEC 27001 untuk menyelesaikan prmasalahan yang ditemukan.

2. Pengumpulan Data

   Tahapan selanjutnya adalah melakukan pengumpulan data dengan pengisian kuesioner Indeks KAMI yang dilakukan oleh responden yang telah dipilih (*staff* IT yang bertanggung jawab) sesuai dengan kategori kuesioner. Kuesioner Indeks KAMI yang digunakan adalah versi terbaru yaitu 4.1.

3. Validasi Data

   Tahap selanjutnya adalah validasi data dengan mengkonfirmasi kepada staff IT terkait untuk memastikan data yang diberikan sesuai dengan keadaan aslinya. Konfirmasi data ini dilakukan secara online menggunakan aplikasi *Zoom Meeting* dengan responden dan meminta bukti berupa dokumen terkait (jika ada) pada setiap area.

4. Analisis Data

   Analisis data merupakan langkah untuk dilakukannya perhitungan hasil kuisioner dan menganalisis tingkat kesiapan (kelengkapan dan kematangan) keamanan informasi pada Instansi/Perusahaan.

5. Hasil dan Pembahasan

   Tahap selanjutnya adalah mempresentasikan hasil dengan melakukan FGD dengan Instansi/Perusahaan

6. Kesimpulan

   Tahapan terakhir adalah penarikan kesimpulan dari hasil penelitian yang dilakukan. Hasil tersebut kemudian dibandingkan dengan kontrol pada ISO 27001. Setelah itu, proses selanjutnya adalalah proses rekomendasi guna memberikan masukan terhadap kekurangan yang belum dilakukan oleh Instansi/Perusahaan.

KELEBIHAN PENILAIAN INDEKS KEAMANAN INFORMASI

1. Indeks keamanan informasi sudah digunakan di Indonesia dan sudah terstandarisasi.
2. Indeks keamanan informasi dapat digunakan untuk meminimalisir adanya ancaman atau risiko pada Instansi/Perusahaan.

MATERI PENILAIAN KEAMANAN INFORMASI

Keamanan informasi adalah upaya untuk mengamankan aset informasi terhadap ancaman yang mungkin timbul (Wijatmoko, 2020). Tata kelola informasi bertanggungjawab untuk memastikan bahwa risiko dikelola dengan tepat dan memverifikasi sumber daya perusahaan digunakan secara bertanggungjawab (Riswaya et al., 2020).

Indeks KAMI merupakan alat evaluasi yang digunakan untuk menganalisis tingkat kesiapan pengamanan informasi di instansi pemerintah (Wowor et al., 2018). Indeks KAMI ini dapat digunakan oleh organisasi dengan skala nasional, maupun yang berukuran kecil. Penggunaan di Instansi pemerintah dapat dilakukan di tingkat pusat maupun satuan kerja yang ada di tingkatan Direktorat Jenderal, Badan, Pusat atau Direktorat untuk mendapatkan gambaran mengenai kematangan program kerja keamanan informasi yang dijalankannya. Evaluasi ini dianjurkan untuk dilakukan oleh pejabat yang secara langsung bertanggungjawab dan berwenang untuk mengelola keamanan informasi di seluruh cakupan instansinya.

Proses evaluasi dilakukan melalui sejumlah pertanyaan di masing-masing area di bawah ini:

- Kategori Sistem Elektronik yang digunakan Instansi
- Tata Kelola Keamanan Informasi
- Pengelolaan Risiko Keamanan Informasi
- Kerangka Kerja Keamanan Informasi
- Pengelolaan Aset Informasi, dan
- Teknologi dan Keamanan Informasi
- Suplemen: Area evaluasi untuk aspek Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan, Pengamanan Layanan Infrastruktur Awan (Cloud Service) dan Perlindungan Data Pribadi.

Pertanyaan yang ada belum tentu dapat dijawab semuanya, akan tetapi yang harus diperhatikan adalah jawaban yang diberikan harus merefleksikan kondisi penerapan keamanan informasi SESUNGGUHNYA.

RENCANA KELANJUTAN PENELITIAN

Selanjutnya, sesuai rekomendasi Indeks KAMI, perlu pengukuran ulang pada semester berikutnya.

REFERENSI

BSSN. (2019). Indeks Keamanan Informasi (Kami). *Badan Siber dan Sandi Negara (BSSN), November*.

Haries Anom Suseyto Aji Nugroho, W. W. W. S. (2019). Metode Silogisme and Untuk Validitas Jawaban Dari Responden Dalam Analisis Maturity Level Keamanan Informasi Berbasis Sni Iso 27001:2013 Pada Dinas Kependudukan Dan Pencatatan Sipil Kota Xyz. *Jurnal Transformasi*, *14*(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, Vol. 14, No. 1, Juni 2020, 10-18 ISSN (print): 1978-9629, ISSN (online): 2442-4943*, *14*(1), 10–18.

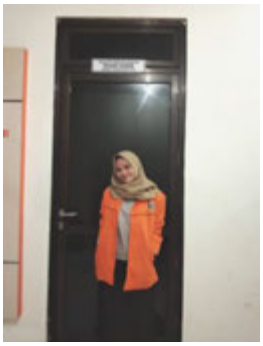
WIJATMOKO, T. E. (2020). Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) Pada Kantor Wilayah Kementerian Hukum Dan Ham Diy. *Cyber Security dan Forensik Digital*, *3*(1), 1–6. https://doi.org/10.14421/csecurity.2020.3.1.1951

Wowor, N. E., Sentinuwo, S. R., Karouw, S. D. S., Elektro, T., Sam, U., Manado, R., Kampus, J., & Bahu, U. (2018). Analisa Keamanan Informasi Pemerintah Kota Manado Menggunakan Indeks Kami. *Jurnal Teknik Informatika*, *13*(3), 1–10. https://doi.org/10.35793/jti.13.3.2018.28081

TENTANG PENULIS

Tawar, S.Si, M.Kom lahir di Klaten pada tanggal 15 April 1971 merupakan alumni Program Studi Ilmu Komputer Universitas Gadjah Mada baik S1 maupun S2. Saat ini bekerja sebagai dosen di Program Studi Sistem Informasi Universitas Ahmad Dahlan Yogyakarta. Selain tugas utama sebagai dosen, punya pengalaman mengelola Biro sistem Informasi dan Komunikasi di universitas yang sama (2008 – 2020) dan saat ini sedang mengemban amanah sebagai Kepala Bidang Pengembangan Pusat Data dan Informasi. Penelitian yang dilakukan adalah pada bidang e-governance dan tata kelola teknologi informasi.

Dr. Imam Riadi, S.Pd., M.Kom lahir di Kudus pada tanggal 10 Agustus 1980 merupakan alumni S1 Pendidikan Teknik Elekto, Universitas Negeri Yogyakarta serta S2,S3 Ilmu Komputer, Universitas Gadjah Mada. Saat ini bekerja sebagai dosen di Program Studi Sistem Informasi dan Magister Informatika Universitas Ahmad Dahlan Yogyakarta.



Adiniah Gustika Pratiwi lahir di Metro, Lampung pada tanggal 26 Agustus 2000 yang merupakan salah satu mahasiswa angkatan 2018 dari Universitas Ahmad Dahlan dengan program studi Sistem Informasi. Ia pernah mengikuti beberapa kegiatan kepanitiaan dan ia juga pernah mengikuti program magang di Technophoria Indonesia.

Ariqah Adliana Siregar lahir di Medan 12 Mei 2000 merupakan salah satu mahasiswa angkatan 2018 di Universitas Ahmad Dahlan dengan program studi Sistem Informasi. Ia pernah menjadi anggotanya Badan Eksekutif Mahasiswa Fakultas Sains dan Teknologi Terapan TA 2018/2019 juga menjadi panitia kegiatan Program Pengenalan Kampus TA 2018/2019. Ia juga pernah mengikuti kegiatan magang di Ruang Ekspresi SI-UAD.

Submit your Paper

International Journal of Advanced Computer Science and Applications

Thank You !

Your paper submission titled "Analysis of Information Security on Chari
Index 4.1" has been received.

You will receive an email confirmation within next 24-48 hours from

Please do add our email address editorijacsa@thesai.org to your Ad
receiving our emails in your inbox

Submission By E-Mail

BACK TO TOP

COMPUTER SCIENCE JOURNAL

About the Journal

Call for Papers

Submit Paper

Indexing

OUR CONFERENCES

Computing Conference

Intelligent Systems Conference

Future Technologies Conference

Communication Conference

HELP & SUPPORT

Contact Us

About Us

Terms and Conditions

Privacy Policy

Analysis of Information Security on Charity Crowdfunding Services using KAMI Index 4.1

Tawar[1], Imam Riadi[2], Ariqah Adliana Siregar[3], Adiniah Gustika Pratiwi[4]
Department of Information System, Universitas Ahamd Dahlan Yogyakarta, Indonesia[1,2,3,4]

Abstract— Technological developments are multiplying. The ABC charity currently has a crowdfunding service. This service helps simplify the user management process. Security is a crucial issue to support and guarantee funders. This research aims to evaluate and provide recommendations for crowdfunding services to run safely and smoothly using the KAMI Index 4.1. This research consists of several steps, starting with observations made at charitable institutions. The following process is through focus group discussion activities to assess the level of information security of crowdfunding services. The analysis of the calculation results is used as the basis for developing recommendations. Based on the assessment results, crowdfunding services at charities obtained scores of I to I+, this indicates that the charity is still in its initial condition and has not yet implemented information security standards in managing crowdfunding services. Recommendations proposed to increase the value are carried out by compiling and implementing information security at the charity.

Keywords— Assessment; Information; KAMI Index; Security; Crowdfunding.

I. INTRODUCTION

Information and Communication Technology (ICT) development is currently experiencing rapid development [1]. Supported by computer networks, these technological advances allow information to be interwoven easily and quickly by anyone and anywhere. In Indonesia today, many organizations, both private and government, take advantage of the development of information technology [2]. The influence of Information and Communication Technology has made it an essential asset for individuals, the private sector, and the government [3].

Information is a valuable asset for organizations and agencies. This information becomes easy to attack or exploit by irresponsible parties [4]. Based on this, the organization or agency must be aware of information security related to integrity, availability, and confidentiality [5].

In an agency or organization that has utilized technology in business processes, it is necessary to have good governance. Information security is an important aspect and needs to be notice [6], believing that government will directly impact the organization because the government will hampered if a main object experiences problems, threats, damage, disruption, theft, and loss [7]. The National Standardization Agency (BSN) said that in implementing public services, good governance is needed, which discusses transparency, efficiency, accountability, and effectiveness in IT benefits. It is also explained in the Minister of Communication and Information (KOMINFO) Number 41 of 2007, which contains general guidelines for managing national Information and Communication Technology. This indicates that Information Technology Governance is crucial in implementing IT services [8].

One organization that has used information technology is Charity Organization ABC. Charity Organization ABC is a national-level zakat institution responsible for managing zakat funds, waqf, infaq, qurban and philanthropic funds [9]. The establishment of Charity Organization ABC is intended as a zakat management institution with modern management that delivers zakat as part of solving social problems (problem solvers) that continue to develop in society [10]. In fulfilling this program, Charity Organization ABC has created an IT-based system to support its business processes, even though some platforms have not run optimally. One of these platforms is fundraising using the crowdfunding method. This method has a positive impact, namely making it easier for a person or organization to search for funds and a negative impact in the form of the vulnerability of the crowdfunding method to cybercrime and still being digitized in Charity Organization ABC, so there are still minimal policies related to information security in the crowdfunding system.

The Minister of Communication and Information (KOMINFO) issued regulation No. 4 of 2016 related to the Technology Security Management System, explaining that every electronic system operator is required to carry out the security of information in the public interest, public services, and the smooth implementation of national security and defense [11]. As a form of implementation of the applicable law, the Ministry of Communication and Information of the Republic of Indonesia hopes that every organization that uses electronic systems can carry out certifications related to information security. Therefore, it is necessary to carry out an assessment related to how information security is implemented in an organization. Several assessment tools can be used related to information security in educational institutions and public

service organizations, for example by using ISO 27001:2013 [12], COBIT, a combination of COBIT 4.1 [13], ITIL V.3 [14], ISO 27001 [15] and KAMI Index.

The KAMI index is a measuring tool designed to assess and evaluate the level of maturity and completeness of implementation following the ISO/IEC 27001:2013 standard and provides an overview of information security governance within an agency or organization [16]. In its development, the KAMI Index continues to develop from the KAMI Index 1.0 until it was developed by the National Cyber and Crypto Agency (BSSN) to 4.1. There are quite striking differences in version 4.0, namely the addition of an evaluation area related to third parties, cloud services, and personal data protection [17]. At the same time, in the KAMI Index 4.1, there are not too many changes, only revisions and editorial additions by the National Cyber and Crypto Agency (BSSN).

II. Related Works

A. Information Security Information

According to ISO 27001:2005, information security is protection related to information from various threats to minimize business risk, ensure business continuity, and maximize return on investment and business opportunities. Then information security, according to ISO 27001:2013, is an information security management system that maintains the integrity, confidentiality, and availability of information in it, applies risk management processes, and assures interested parties that risks are correctly managed [18].

Information security is applied in organizations to overcome obstacles and problems that arise both technically and non-technically [19]. Figure 1 is information security, which has three aspects: confidentiality, integrity, and availability. Confidentiality is an aspect that ensures that information and data owned by the company can be accessed only by authorized parties. Integrity, an element to maintain accuracy, guarantees that the data held is not modified without the permission of the authorities and the integrity of the information. Integrity as an aspect to maintain accuracy, ensure that the data owned is not modified without the authorities' permission and the integrity of the data [20].

Figure 1. Information Security Elements

B. Information Security Management System (ISMS)

An organization or agency requires an information security management system as a target to achieve the goals of the organization or agency by establishing, using, implementing, reviewing, maintaining, improving information security and minimizing risk, as well as ensuring the business continuity of an organization or agency proactively to limit the impact that will arise from a security breach [21]. Information Security Management System (SMKI) must meet national and international standards that have been developed since 2005 by the International Organization for Standardization (ISO) so that the quality of the security provided can solve existing problems. The application of a process system within an agency and an identification analysis are each process and management are referred to as the "process approach." In the ISMS, the process approach is presented following the ISMS standard based on operating principles adopted from the ISO management system standard, commonly referred to as the Plan-Do-Check-Act (PDCA) process [22]. The following explains the Plan-Do-Check-Act process:

- Plan, n this process, will analyze, set overall goals and targets, also develop plans to achieve them.
- Do, in this process, will implement or carry out the planned plan.
- Check, this process will monitor and measure the extent to which the achievement has met the planned goals.
- Act, this process will improve activities that have not been following the plan, learn from previous mistakes, and enhance activities to achieve better results.

C. Information Technology Risk Management Risk

Risk is a process of activities carried out to determine opportunities for attacks or threats that can cause disruption of business processes and even fail the goals of the agency or organization [23]. Risk management is the process of striking a balance between efficiency and realizing opportunities to gain profits and reduce losses and vulnerabilities [24].

An organization or agency has data or information that is important and is a resource that can increase the value or image of the organization or institution. With this data and information, organizations or agencies need information security. Information security aims to minimize risk, guarantee business processes, protect data from various dangerous threats such as data theft, viruses, and other attacks.

D. ISO/IEC 27001 as an ISMS Standard

ISO/IEC 27001 is an international standard document recommended for implementing an Information Security Management System (ISMS). ISO 27001 is a standard intended to assist organizations or agencies in maintaining and protecting the Information Security Management System (ISMS) and the security of company assets. ISO/IEC 27001 is a framework designed in such a way that it can apply to small and large-scale organizations or agencies that are used to specify the need to create, implement, implement, monitor, analyze, improve management regularly and maintain and document a Management System Information Security (SMKI) [25].

E. Information Security Index version 4.1 as an ISMS tool

The KAMI index is a tool or evaluation tool compiled by the Directorate of Information Security Team of the Ministry of Communication and Information Technology, which is used to analyze, measure, and evaluate the level of readiness for the application of information security in government agencies whose contents have been adjusted to the criteria in SNI ISO/IEC 27001. The KAMI index is not intended to analyze the feasibility or effectiveness of existing forms of security but only as a tool to provide an overview of the condition of readiness, completeness, and maturity and an information security framework in the environment for organizational leaders or agencies.

Organizations or agencies can use the KAMI index on a national and small scale. The evaluation of the KAMI Index is recommended to be carried out by staff or officials who have the responsibility and authority to manage information security within the organization or agency. In the KAMI Index, the items to be evaluated focus on five areas, namely Electronic Systems, Governance, Risk Management, Asset Management, Technology and Information Security [26].

Before the quantitative assessment process, the initial stage is to carry out a classification process for the Electronic System used by the agency or organization to classify the Electronic System used into a certain "level" or "size." The results obtained mean the dependence of an organization or agency on the role of Electronic Systems. Figure 2 shows the final score that will be customized just to the readiness status of the agency or organization for information security.

Elelctronic System Categori				
Low		Final Score		Readiness Status
10	15	0	174	Not Feasible
		175	312	Fulfillment of the basic framework
		313	535	Pretty good
		536	645	Good
High		Final Score		Readiness Status
16	34	0	272	Not Feasible
		273	455	Fulfillment of the basic framework
		456	583	Pretty good
		584	645	Good
Strategic		Final Score		Readiness Status
35	50	0	333	Not Feasible
		334	535	Fulfillment of the basic framework
		536	609	Pretty good
		610	645	Good

Figure 2. SE Category Matrix with KAMI Index Readiness Status

Each category has questions based on readiness to implement and secure information security following the ISO/IEC 27001:2013 standard. The grouping is explained as follows:

- Label “1” from the basic framework of information security
- Label “2” form of consistency and effectiveness of the application of information security.
- Label “3” form of ability to improve information security performance following the minimum prerequisite readiness standards for ISO/IEC 27001:2013 certification.

In having different assessment weights according to the completeness control label. Figure 3 is the score for each label .

	Security Status		
Security Status	1	2	3
Not done	0	0	0
In planing	1	2	3
In progress	2	4	9
Fully applied	3	6	6

Figure 3. The score value of control completeness label

Questions categorized by maturity level and applicability refer to the maturity level used by COBIT or CMMI. Maturity level is described as follows:

- Level I - Initial Condition
- Level II - Implementation of the Basic Framework
- Level III - Defined and Consistent
- Level IV - Managed and Scalable
- Level V – Optimal

The KAMI index makes it easier to provide detailed descriptions with I+, II+, III+ and IV+ details. The minimum standard in readiness for certification in ISO/IEC 27001:2013 is at level III+. Figure 4 relates the level of security completeness (bottom) and maturity of experience (top).

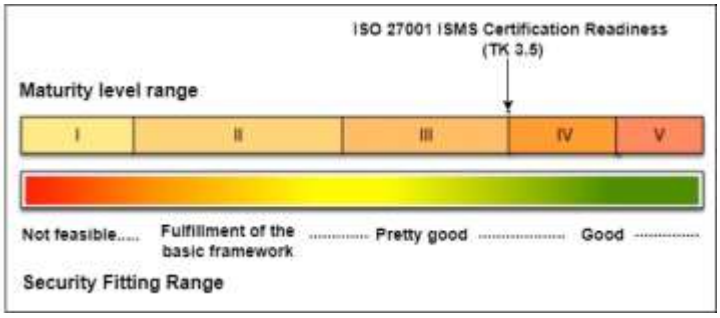


Figure 4. Maturity Level and Completeness of Security

III. RESEARCH METHOD

This research assesses the level of information security in an organization using KAMI Index 4.1 method. Figure 5 depicts the research flow and the following explanation:

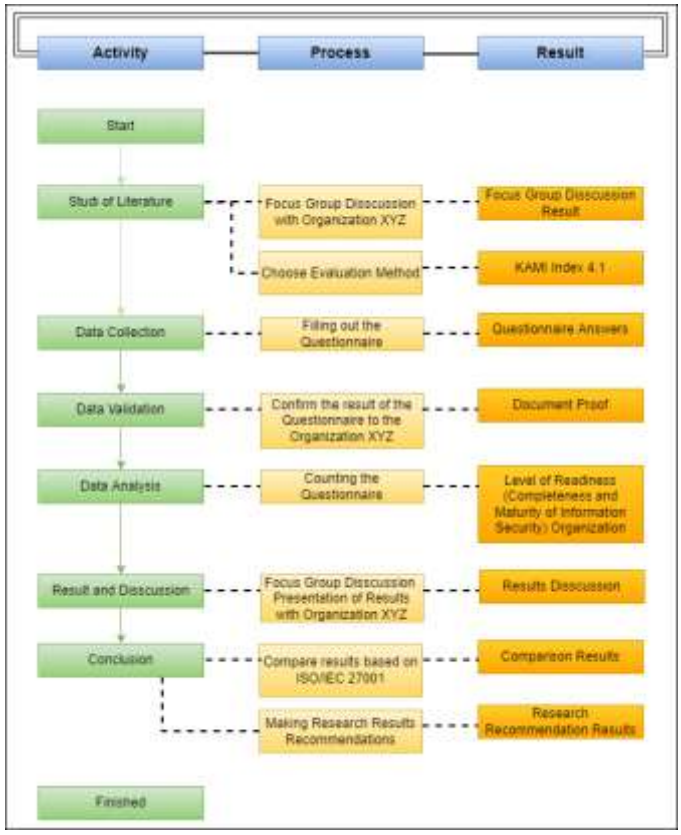


Figure 5. Research Stages of KAMI Index

A. Focus Group Discussion (FGD)

At the literature study stage, the author identified problems with FGD activities with Charity Organization ABC, especially the IT section on the crowdfunding system. It found that Charity Organization ABC uses Information Technology in its business processes. Several platforms are not yet running effectively and are still in the development stage. In this crowdfunding system, information security evaluation has never been done. Then the author chooses the evaluation method of the KAMI Index Version 4.1, which follows the ISO/IEC 27001:2013 standard.

B. Data collection

Data Collection The data collection stage is carried out through FGD using the KAMI Index evaluation tool, which is filled in directly by the IT staff of the Charity Organization ABC crowdfunding system. The questionnaire has been filled in the questionnaire for all categories in the KAMI Index Version 4.1.

C. Data validation

At the data validation stage, the researcher confirmed the results of the answers carried out in the previous step to the IT staff and attached evidence of the related documents. The purpose of this stage is to verify that the data given is following the actual situation.

D. Data analysis

At the data analysis stage, the researcher begins to process the results that have been confirmed in the previous step. Researchers analyzed and calculated the questionnaire according to the KAMI Index formula Version 4.1

E. Results and Discussion

At this stage the researcher has obtained, confirmed, processed, analyzed and made recommendations following the results obtained. Then the researcher will present the results and recommendations to Charity Organization ABC.

F. Conclusion

The conclusion the results is the last stage in the research flow. At this stage, the authors make conclusions by comparing the evaluation results following the control by ISO 27001 and make recommendations according to the results obtained.

IV. RESULT AND DISCUSSION

Research the maturity level of information security on the Charity Organization ABC crowdfunding system using the KAMI Index evaluation tool 4.1. The KAMI index has 194 questions divided into seven sections. A series of studies have been carried out, and the evaluation results are shown in Figure 6. In the radar diagram picture x, the diagram that forms the orange line pattern is the condition of the SMKI in Charity Organization ABC based on the results of filling out the questionnaire by the informants.

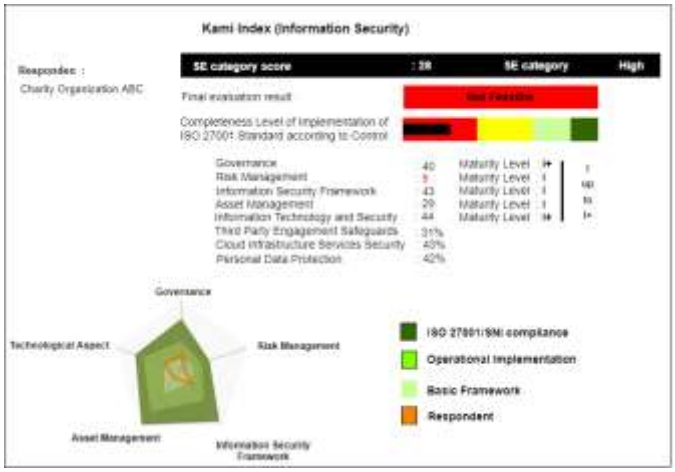


Figure 6. Evaluation Results Dashboard

A. Electronic System Category

The The Electronic System category is the first category in the KAMI Index that evaluates the electronic system level used. In the category of electronic systems, there are three categories of results, namely low, high and strategic. The electronic system category has ten questions with a maximum score of 50. The results obtained in the Electronic System category based on the WE Index assessment obtained a score of 28, so that will can include it in the high category according to the maturity

level table of the KAMI Index where the High category ranges from a score of 16 to 34, as an assessment guide can be seen in table 1.

Table 1. Electronic System Category Score

Electronic System Category Score	
Low	10-15
High	16-34
Strategic	35-50

Figure 7. Total Results in the Electronic System Category

B. Information Security Governance Category

The Governance category is the second category in the KAMI Index that evaluates the level of governance in the system used. The Information Security Governance assessment in the crowdfunding system at Charity Organization ABC received a total Information Security Governance evaluation score of 40 out of 22 questions with a maturity level status of I+. The minimum threshold for certification readiness for the expected maturity level is Level III+. Still, the information security governance results obtained are only valid at the maturity level I+, which means they are in the initial condition level. Based on table 2, information security management in the crowdfunding system, there is a reasonably large understanding of information security within the agency, documenting every task and responsibility for managing information security and maintaining compliance and has not defined a policy of criminal action against information security incidents.

Table 2. Evaluation Results of the Governance Category

Security Status	Maturity level						Total
	1	SC	2	SC	3	SC	
Not done	0	0	0	0	0	2	0
In planning	1	2	2	3	3	3	8
In progress	2	5	4	4	6	1	26
Fully applied	3	0	6	1	9	0	6
Total score							**40**

C. Information Security Risk Management Category

The Risk Management category is the third category in the KAMI Index, which evaluates the level of risk in the system used. Information Security Risk Assessment in the crowdfunding system at Charity Organization ABC obtained a total Information Security Risk evaluation score of 9 out of 16 questions with maturity level I. Information Security Risk Management in the crowdfunding system is valid at maturity level I, which means it is initial. This system already understands the need for information security management, and it needs to be improved. Based on table 3, Information security risks in the crowdfunding system need to identify threats and weaknesses related to information assets, develop risk mitigation and mitigation measures, carry out periodic risk mitigation checks, conduct regular assessments of the risk management framework to ensure/improve its effectiveness. Table 3. Risk category evaluation results

Table 3. Evaluation Results of the Security Risk Category

Security Status	Maturity level						Total
	1	SC	2	SC	3	SC	
Not done	0	2	0	4	0	0	0
In planning	1	7	2	0	3	0	7
In progress	2	1	4	0	6	0	2
Fully applied	3	0	6	0	9	0	0
Total score							**9**

D. Categories of Information Security Management Framework

The framework category is the fourth category in the KAMI Index that evaluates the framework on the system used. Assessment of the Information Management Framework in the crowdfunding system at Charity Organization ABC received a total evaluation score of 43 out of 29 questions with maturity level I status. The Information Management Framework area is at maturity level I, which means it is in the initial condition. Based on table 4, the information security framework on the crowdfunding system needs to determine a secure system development policy it is necessary to control information system audits and verify review and evaluate the continuity of information security.

Table 4. Evaluation Results of the Framework Category

Security Status	Maturity Level						Total
	1	SC	2	SC	3	SC	
Not done	0	3	0	4	0	2	0
In planning	1	4	2	0	3	2	4
In progress	2	2	4	2	6	1	12
Fully applied	3	1	6	4	9	2	27
Total score							**43**

E. Information Asset Management Category

The Asset Management category is the fifth category in the KAMI Index that evaluates asset management on the system used. The Management of Information Assets assessment in the crowdfunding system at Charity Organization ABC obtained a total evaluation value of 29 out of 38 questions with maturity level status I. In the area of Information Asset Management, it is valid at maturity level I, which means it is in the initial condition. Based on table 5, Information Security Asset Management in the crowdfunding system needs to protect all assets (offices, rooms, and facilities) from external

environmental threats, ensure the procedures for intellectual property rights and access security used.

Table 5. Evaluation results of Asset Management Category

Security Status	Maturity Level						Total
	1	SC	2	SC	3	SC	
Not done	0	13	0	7	0	3	0
In planning	1	3	2	1	3	1	5
In progress	2	8	4	2	6	0	24
Fully applied	3	0	6	0	9	0	0
Total score							**29**

F. Information Technology and Security Category

The Information Security Technology category is the sixth category in the KAMI Index that evaluates the technology in the system used. The assessment of Information Security and Technology Management in the crowdfunding system at Charity Organization ABC obtained a total value of the Information Technology and Security evaluation of 44 out of 26 questions with a maturity level status of I+. In the area of Technology and Information Security, it is valid at maturity level I, which means it is in the initial condition. Based on table 6, information security technology in the crowdfunding system needs to control malware and networks.

Table 6. Evaluation Results for the Category of Information Technology and Security

Security Status	Maturity Level						Total
	1	SC	2	SC	3	SC	
Not done	0	5	0	4	0	2	0
In planning	1	1	2	1	3	0	3
In progress	2	7	4	3	6	0	26
Fully applied	3	1	6	2	9	0	15
Total score							**44**

G. Supplement Category

The Supplement Category is the seventh or final category on the KAMI Index. The results of the evaluation at the supplement stage obtained that the maturity level for securing third-party involvement was 31%. Then for the security of cloud infrastructure services by 43% and the last is personal data protection by 42%. The score obtained from the calculation of this supplement category does not affect the total score from part I to part VI in the US Index assessment, which indicates the level of readiness and maturity of information security. Based on the KAMI index, the assessment of this supplement category aims to detect the emergence of new information security risks with the involvement of these three aspects.

V. CONCLUSION

The assessment results of the level of use of Electronic Systems are 32 out of a total of 50. This shows that the crowdfunding system has entered the high category in electronic systems, which means that electronic systems are an inseparable part of the work process running on Charity organizations. The order of maturity levels from the lowest to the highest is I – V. The minimum limit to carry out ISO 27001 certification is III+. For now, the maturity level of the Crowdfunding System at Charity Organization Pusat is only limited to I to I+, and the security level of the information system is at the Initial Condition level.

The recommended National Cyber and Crypto Agency (BSSN) research is carried out twice a year. The focus of the following analysis should be able to assess organizational information security using other frameworks to produce data to support corporate information security.

ACKNOWLEDGMENT

Thank you to Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) Universitas Ahmad Dahlan who have provided funding for this research activity through Skema Penelitian Unggulan Program Studi (PUPS) in 2021 based on contract number PUPS-278/SP3/LPPM-UAD/VI/2021.

REFERENCES

[1] M. Yunella, A. D. Herlambang, and W. H. N. Putra, "Evaluation of Information Security Governance at the Malang City Communication and Information Office Using KAMI Index," ... *Teknol. Inf. dan ...*, vol. 3, no. 10, pp. 9552–9559, 2020, [Online]. Available: http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/6521.

[2] A. F. Manullang, C. Candiwan, and L. D. Harsono, "Information Security Assessment Using the Information Security Index (KAMI) at XYZ Institution," *Journal of Information Engineering and Educational Technology*, vol. 1, no. 2. p. 73, 2017, doi: 10.26740/jieet.v1n2.p73-82.

[3] M. R. Slamet, F. Wulandari, and D. Amalia, "Assessment of Technology Security in Electronic Learning Systems Using the Information Security Index at Batam State Polytechnic," *J. Appl. Bus. Adm.*, vol. 3, no. 1, pp. 162–171, 2019, doi: 10.30871/jaba.v3i1.1305.

[4] T. Informatika, U. Sam, R. Manado, J. Kampus, and U. Bahu, "Implementation of KAMI Index at Sam Ratulangi University," *J. Tek. Inform.*, vol. 12, no. 1, 2017, doi: 10.35793/jti.12.1.2017.17869.

[5] F. H. Purwanto and M. Huda, "Measurement of XYZ College Information Security Level Using Information Security Index (KAMI) Based on ISO/IEC-27001: 2013," *J. VOI (Voice Informatics)*, no. 4, pp. 31–40, 2019, [Online]. Available: https://voi.stmik-tasikmalaya.ac.id/index.php/voi/article/view/162.

[6] J. Tukad and B. No, "Information Technology Security Level Assessment Using Information Security Methods (WE) And Vulnerability Assessment," *Jutisi J. Ilm. Tek. Inform. dan Sist. Inf.*, vol. 9, pp. 173–184, 2020.

[7] T. E. WIJATMOKO, "Evaluation of Information Security Using the Information Security Index (US) at the Regional Office of the Ministry of Law and Human Rights DIY," *Cyber Secur. dan Forensik Digit.*, vol. 3, no. 1, pp. 1–6, 2020, doi: 10.14421/csecurity.2020.3.1.1951.

[8] A. R. Riswaya, A. Sasongko, and A. Maulana, "Evaluation of Information Technology Security Governance Using Our Index for Preparation of Standard SNI Iso/Iec 27001 (Case Study: STMIK Mardira Indonesia)," *J. Comput. Bisnis, Vol. 14, No. 1, Juni 2020, 10-18 ISSN 1978-9629, ISSN 2442-4943*, vol. 14, no. 1, pp. 10–18, 2020.

[9] M. Ifas, "Publication Analysis And Financial Statements Based On Psak No. 45 (Case Study Of Lazismu Menteng Jakarta Pusat)," *J. Ekon. Islam*, vol. 9, no. November 2018, pp. 46–74, 2018.

[10] R. A. Izdihar and T. Widiastuti, "The Role of the Surabaya Muhammadiyah Amil Zakat Institution (Lazismu) in Empowering Women MSMEs in Surabaya through the Utilization of Infaq and Shadaqah Funds," *J. Ekon. Syariah Teor. dan Terap.*, vol. 6, no. 3, p. 525, 2020, doi: 10.20473/vol6iss20193pp525-540.

[11] S. I. D. Octaviani, Suprapto, and A. D. Herlambang, "Evaluation of the Readiness of the Information Security Framework at the Batu City Communications and Information Office Using KAMI Index," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 3, pp. 2741–2745, 2019.

[12] H. Hambali and P. Musa, "Analysis of Governance Security Management Information System Using Index Kami in Central Government Institution," *Angkasa J. Ilm. Bid. Teknol.*, vol. 12, no. 1, 2020, doi: 10.28989/angkasa.v12i1.563.

[13] D. Ariyadi, H. Kusbandono, and I. P. Astuti, "Recommendations for IT Infrastructure Improvement in Vocational High Schools Based on Maturity Level Evaluation with Cobit 4.1 Framework," *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 3, no. 1, p. 80, 2019, doi: 10.30645/j-sakti.v3i1.90.

[14] R. D. Pribadi, Y. Herry, A. I. Hadiana, and W. Witanti, "Measurement of Maturity Level of Information Technology Based on Itil V.3 at Jenderal Achmad Yani University" *J. Ilm. Teknol. Inf. Terap.*, vol. IV, no. 1, pp. 11–17, 2017.

[15] A. Fathurohman and R. W. Witjaksono, "Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using ANNEX Control (Case Study: District of Government of Bandung City)," *Bull. Comput. Sci. Electr. Eng.*, vol. 1, no. 1, pp. 1–11, 2020, doi: 10.25008/bcsee.v1i1.2.

[16] E. R. Pratama, Suprapto, and A. R. Perdanakusuma, "Evaluation of Information Technology Security System Governance Using the KAMI Index and ISO 27001: A Case Study of KOMINFO East Java Province," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 11, pp. 5911–5920, 2018, [Online]. Available: http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/3465.

[17] N. Luh, P. Ning, and S. Putri, "E-Government Information Security Assessment Using the Information Security Index (KAMI) 4 . 0," *J. Teknol. Inf. dan Komput.*, vol. 6, no. 2, pp. 238–244, 2020.

[18] Y. C. Yuze, Y. Priyadi, and . C., "Analysis of Information Security Management Systems Using ISO/IEC 27001: 2013 And Recommendation System Models Using Data Flow Diagrams at the Directorate of Higher Education Information Systems," *J. Sist. Inf. Bisnis*, vol. 6, no. 1, p. 38, 2016, doi: 10.21456/vol6iss1pp38-45.

[19] R. Umar, I. Riadi, and E. Handoyo, "Information System Security Analysis Based on COBIT 5 Framework Using Capability Maturity Model Integration (CMMI)," *J. Sist. Inf. Bisnis*, vol. 9, no. 1, p. 47, 2019, doi: 10.21456/vol9iss1pp47-54.

[20] N. A. Widodo and and A. F. R. , R. Rizal Isnanto, "Information Security Management System Planning And Implementation Based ON ISO/IEC 27001:2005 STANDARDS (Case Study in a National Private Bank)," vol. 4, no. 1, pp. 60–66, 2016.

[21] A. C. D. Tinungki, S. R. Sentinuwo, and S. Karouw, "Analysis of the Maturity Level of Information Security Implementation by the Bitung City Government Using the KAMI Index (Case Study: Communication and Information Office) ," *Repo.Unsrat.Ac.Id*, pp. 1–8, 2021, [Online]. Available: http://repo.unsrat.ac.id/2963/.

[22] W. Apriandari and A. Sasongko, "Information Security Management System Analysis Using Sni Iso / Iec 27001: 2013 in the Regional Government of Sukabumi City (Case Study: At Diskominfo Sukabumi City)," *Ilm. SANTIKA*, vol. 8, no. 1, pp. 715–729, 2018.

[23] A. Asriyanik and Prajoko, "Information Security Management in Academic Information Systems Using ISO 27005:2011 on Academic Information Systems (SIAK) Universitas Muhammadiyah Sukabumi (UMMI)," *J. Tek. Inform. dan Sist. Inf.*, vol. 4, no. 2, pp. 315–325, 2018.

[24] N. Matondang, I. N. Isnainiyah, and A. Muliawatic, "Analysis of Information System Data Security Risk Management (Case Study: XYZ Hospital)," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 2, no. 1, pp. 282–287, 2018, doi: 10.29207/resti.v2i1.96.

[25] W. C. Pamungkas and F. T. Saputra, "Evaluation of Information Security at SMA N 1 Sentolo Based on the Information Security Index (KAMI) ISO/IEC 27001:2013," *J. Sist. Komput. dan Inform.*, vol. 1, no. 2, p. 101, 2020, doi: 10.30865/json.v1i2.1924.

[26] M. I. Rosadi and L. Hakim, "Yudharta University SIAKAD Safety Measurement and Evaluation Using the KAMI Index," *Explor. IT J. Keilmuan Apl. Tek. Inform. Univ. Yudharta Pasuruan*, vol. 7, no. 1, pp. 33–42, 2015.

JUITA Jurnal Informatika
e-ISSN: 2579-8901
p-ISSN: 2086-9398
http://jurnalnasional.ump.ac.id/index.php/juita

#12695 SUMMARY

Summary (http://jurnalnasional.ump.ac.id/index.php/JUITA/author/submission/12695) | Review (http://jurnalnasional.ump.ac.id/index.php/JUITA/author/submissionReview/12695) | Editing (http://jurnalnasional.ump.ac.id/index.php/JUITA/author/submissionEditing/12695)

SUBMISSION

Authors	Tawar Tawar, Imam Riadi, Adiniah Gustika Pratiwi, Ariqah Adliana Siregar
Title	Assessment and Mitigation of Information Security Policy in Budgeting System for Charity Organization XYZ using KAMI Index 4.1
Original file	12695-33611-1-SM.docx (http://jurnalnasional.ump.ac.id/index.php/JUITA/author/downloadFile/12695/33611/1) 2022-01-03
Supp. files	None Add a Supplementary File (http://jurnalnasional.ump.ac.id/index.php/JUITA/author/addSuppFile/12695)
Submitter	Mr. Tawar Tawar (http://jurnalnasional.ump.ac.id/index.php/JUITA/user/email?to%5B%5D=Mr.%20Tawar%20Tawar%20%3Ctawar%40is.uad.ac.id%3E&redirectUrl=http%3A%2F%2Fjurnalnasional.ump.ac.id%2Findex.php%2FJUITA%2Fauthor%2Fsubmission%2F12695&subject
Date submitted	January 3, 2022 - 09:54 PM
Section	JUITA
Editor	None assigned
Author comments	I hope this manuscript will be accepted anda published in JUITA.

STATUS

Status	Awaiting assignment
Initiated	2022-01-03
Last modified	2022-01-03

SUBMISSION METADATA

Edit Metadata (http://jurnalnasional.ump.ac.id/index.php/JUITA/author/viewMetadata/12695)

Authors

Name	Tawar Tawar (http://jurnalnasional.ump.ac.id/index.php/JUITA/user/email?redirectUrl=http%3A%2F%2Fjurnalnasional.ump.ac.id%2Findex.php%2FJUITA%2Fauthor%2Fsubmission%2F12695&to%5B%5D=Tawar%20Tawar%20%3Ctawar%4
Affiliation	Universitas Ahmad Dahlan
Country	Indonesia
Bio Statement	Department of Information System
Principal contact for editorial correspondence.	
Name	Imam Riadi (http://jurnalnasional.ump.ac.id/index.php/JUITA/user/email?redirectUrl=http%3A%2F%2Fjurnalnasional.ump.ac.id%2Findex.php%2FJUITA%2Fauthor%2Fsubmission%2F12695&to%5B%5D=Imam%20Riadi%20%3Cimam.riad
Affiliation	Universitas Ahmad Dahlan
Country	Indonesia
Bio Statement	Department of Information System
Name	Adiniah Gustika Pratiwi (http://jurnalnasional.ump.ac.id/index.php/JUITA/user/email?redirectUrl=http%3A%2F%2Fjurnalnasional.ump.ac.id%2Findex.php%2FJUITA%2Fauthor%2Fsubmission%2F12695&to%5B%5D=Adiniah%20Gustika%20Pratiwi%2
Affiliation	Universitas Ahmad Dahlan
Country	Indonesia
Bio Statement	Department of Information System
Name	Ariqah Adliana Siregar (http://jurnalnasional.ump.ac.id/index.php/JUITA/user/email?redirectUrl=http%3A%2F%2Fjurnalnasional.ump.ac.id%2Findex.php%2FJUITA%2Fauthor%2Fsubmission%2F12695&to%5B%5D=Ariqah%20Adliana%20Siregar%2C
Affiliation	Universitas Ahmad Dahlan
Country	Indonesia
Bio Statement	Department of Information System

Title and Abstract

Title	Assessment and Mitigation of Information Security Policy in Budgeting System for Charity Organization XYZ using KAMI Index 4.1
Abstract	**Threats to information resources require information security management policies in every agency. The Information Security Index (KAMI Index) is one of the methods developed by the Ministry of Communication and Information Technology, used to evaluate the maturity level, completeness of ISO/IEC 27001:2013 implementation and information security readyness. As a national zakat institution, XYZ Organization has utilized information technology in several systems, including the budgeting system. However, the information security index has never been measured. This condition may result in the risk of threats to information security, so it is necessary to measure. The Budgeting System needs to be measured using KAMI Index 4.1. The assessment criteria are carried out on seven categories to know how the quality of the information security policy is. The results of this assessment, XYZ organization gets an electronic system score is 17, governance 75, risk management 30, framework 31, asset management 37, ICT 38, securing third party involvement 40%, service security 20%, personal data protection 27% so the total score of 5 categories is 211 or at level I+ to II. This organization has started implement the framework at early stage and has not met the initial requirements for ISO/IEC 27001:2013 certification.**

Indexing

Academic discipline and sub-disciplines	Information System;
Keywords	Assessment; Information; KAMI Index; Security; Zakat Institution
Language	en

Supporting Agencies

Agencies	—

References

References

[1] E. R. Pratama, Suprapto, dan A. R. Perdanakusuma, "Evaluation of Information Technology Security System Governance Using the KAMI Index and ISO 27001: A Case Study of KOMINFO East Java Province," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 11, hal. 5911–5920, 2018, [Daring]. Tersedia pada: http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/3465.

[2] T. Effendy *et al.*, "Evaluation of Information Security Using the Information Security Index (US) at the Regional Office of the Ministry of Law and Human Rights Diy," vol. 3, no. 1, hal. 1–6, 2020.

[3] B. Sutara, "PDAM Titra Medal Information Security Measurement Using the US Index for Information Security Maturity Level Analysis," vol. 17, no. 2, hal. 34–41, 2018, [Daring]. Tersedia pada: https://ejournal.ikmi.ac.id/index.php/jict-ikmi/article/view/32.

[4] Yustanti, W. Rahadian, B. Anita, Q. Prihanto, dan Agus, "Analysis Of Readiness And Maturity Level Of Implementation Of Iso 27001: 2013 Using Information Security Index 3: 2015 At Upt . Ppti State University Surabaya The Ministry of Communication and Information Technology of the Republic of Indonesia has issued regulation number," *Inform. P. T., Inform. J. T., Surabaya, U. N., Hari, D., Bulan, T., Hari, D., Bulan, T. (2016). Anal. Tingkat Kesiapan Dan Kematangan Implementasi Iso 27001 2013 Menggunakan Indeks Keamanan Inf. 3 2015 Pada Upt . Ppti Univ. N*, no. 4, hal. 1602–1613, 2016.

[5] M. R. Slamet, F. Wulandari, dan D. Amalia, "Assessment of Technology Security in Electronic Learning Systems Using the Information Security Index at Batam State Polytechnic," *J. Appl. Bus. Adm.*, vol. 3, no. 1, hal. 162–171, 2019, doi: 10.30871/jaba.v3i1.1305.

[6] W. W. W. S. Haries Anom Suseyto Aji Nugroho, "The syllogism method and for the validity of the answers from respondents in the analysis of the Maturity Level of Information Security Based on Sni Iso 27001:2013 at the Department of Population and Civil Registration of the City of Xyz," *J. Transform.*, vol. 14, no. 2, 2019.

[7] J. F. Andry dan A. K. Setiawan, "It Governance Evaluation Using Cobit 5 Framework on the National Library," *J. Sist. Inf.*, vol. 15, no. 1, hal. 10–17, 2019, doi: 10.21609/jsi.v15i1.790.

[8] Y. Sekhara, H. Medromi, dan H. Nahla, "Multi Agent Decision system for the IT Governance Platform," vol. 15, no. 5, hal. 290–306, 2017.

[9] A. R. Riswaya, A. Sasongko, dan A. Maulana, "Evaluation of Information Technology Security Governance Using Our Index for Preparation of Sni Iso/Iec 27001 Standard (Case Study: Stmik Mardira Indonesia)," *J. Comput. Bisnis, Vol. 14, No. 1, Juni 2020, 10-18 ISSN 1978-9629, ISSN 2442-4943*, vol. 14, no. 1, hal. 10–18, 2020.

[10] N. A. Widodo dan and A. F. R. , R. Rizal Isnanto, "Information Security Management System Planning And Implementation Based On Iso/Iec 27001:2005 StandardS (Case Study in a National Private Bank)," vol. 4, no. 1, hal. 60–66, 2016.

[11] N. E. Wowor *et al.*, "AAnalysis of Manado City Government Information Security Using Our Index," *J. Tek. Inform.*, vol. 13, no. 3, hal. 1–10, 2018, doi: 10.35793/jti.13.3.2018.28081.

[12] T. Hartati, "Information Security Management System Planning in Academic Field Using ISO 27001: 2013," *KOPERTIP J. Ilm. Manaj. Inform. dan Komput.*, vol. 1, no. 2, hal. 63–70, 2017, doi: 10.32485/kopertip.v1i02.24.

[13] F. Febrianto dan D. I. Sensuse, "Evaluation of information security using ISO / IEC 27002: a case study on the Banjarnegara Tunas Bangsa," *Infokam*, vol. 2, no. 2013, hal. 21–27, 2017.

[14] R. C. Annisyah, A. Budiono, dan R. Fauzi, "Analysis And Design Of Information Security Management Directorate Of Information Systems Of Telkom University Using The Information Security Index (Kami) In The Area Of Information Asset Management, Technology And Information Security" vol. 8, no. 2, hal. 2663–2677, 2021.

[15] N. Matondang, I. N. Isnainiyah, dan A. Muliawatic, "Analysis of Information System Data Security Risk Management (Case Study: XYZ Hospital)," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 2, no. 1, hal. 282–287, 2018, doi: 10.29207/resti.v2i1.96.

[16] W. Apriandari dan A. Sasongko, "Information Security Management System Analysis Using Sni Iso / Iec 27001: 2013 in the Regional Government of Sukabumi City (Case Study: At Diskominfo Sukabumi City)," *Ilm. SANTIKA*, vol. 8, no. 1, hal. 715–729, 2018.

[17] R. Adi, P. Pratama, R. Sengkey, dan C. Punusingon, "Information Security Analysis of Southeast Minahasa District Government Using KAMI Index," vol. 15, no. 3, hal. 189–198, 2020.

[18] B. A. Firzah, "Evaluation of Information Security Management Using the Information Security Index (US) Based on Iso / Iec 27001: 2013 at the Directorate of Information Technology and System Development (Dptsi) Its Surabaya Evaluating Information Security Management Using KAMI Index," vol. 6, no. 1, 2017.

[19] H. Hambali dan P. Musa, "Analysis of Governance Security Management Information System Using Index Kami in Central Government Institution," *Angkasa J. Ilm. Bid. Teknol.*, vol. 12, no. 1, 2020, doi: 10.28989/angkasa.v12i1.563.

[20] M. Bakri dan N. Irmayana, "Analysis and Implementation of Simhp Bpkp Information Security Management System Using ISO 27001 Standard," *J. Tekno Kompak*, vol. 11, no. 2, hal. 41, 2017, doi: 10.33365/jtk.v11i2.162.

[21] M. Lenawati, W. W. Winarno, dan A. Amborowati, "Information Security Governance in PDAM Using ISO/IEC 27001:2013 and COBIT 5," *Sentra Penelit. Eng. dan Edukasi*, vol. 9, no. 1, hal. 44–49, 2017, [Daring]. Tersedia pada: http://speed.web.id/jurnal/index.php/speed/article/view/220.

[22] Y. C. Pradipta, Y. Rahardja, M. N. N. Sitokdana, U. Kristen, dan S. Wacana, "Information and Communication Technology of Aviation and Space (Pustikpan) Using Sni Iso / Iec 27001: 2013," hal. 352–358, 2013.

[23] W. C. Pamungkas dan F. T. Saputra, "Evaluation of Information Security at SMA N 1 Sentolo Based on Information Security Index (KAMI) ISO/IEC 27001:2013," *J. Sist. Komput. dan Inform.*, vol. 1, no. 2, hal. 101, 2020, doi: 10.30865/json.v1i2.1924.

[24] D. A. Wati, A. Budiono, dan R. Fauzsi, "Analysis And Design Of Information Security Management In The Directorate Of Telkom University Information Systems With Information Security Index (Us) In Security Governance Area Of Information, Risk Management Of Information Security And Information Framework For Information Security Management," *Αγαη*, vol. 8, no. 5, hal. 55, 2019.

[25] BSSN, "Information Security Index (KAMI Index)," *Badan Siber dan Sandi Negara*, no. November, 2019.

ISSN: 2579-8901

Register (/index.php/JUITA/user/register)

Author Guidelines (/index.php/JUITA/about/submissions#authorGuidelines)

(https://drive.google.com/open?id=1f1l9JXY-Zx7sOwRBuMeigZ3h_JOBv4Ki)

Notifications

View (http://jurnalnasional.ump.ac.id/index.php/JUITA/notification) Manage (http://jurnalnasional.ump.ac.id/index.php/JUITA/notification/settings)

Article Template (https://docs.google.com/document/d/1JoUHP707SsdT_4s6_0tXX6pXiQTmJW-1/edit?usp=sharing&ouid=114837924174631254413&rtpof=true&sd=true)

(https://docs.google.com/document/d/1JoUHP707SsdT_4s6_0tXX6pXiQTmJW-1/edit?usp=sharing&ouid=114837924174631254413&rtpof=true&sd=true)

(https://drive.google.com/file/d/1SodjoRxpn3mlwqVwO6XCT-ItPTwlyrHZ/view?usp=sharing)

User

You are logged in as...
tawar
My Journals (http://jurnalnasional.ump.ac.id/index.php/index/user)
My Profile (http://jurnalnasional.ump.ac.id/index.php/JUITA/user/profile)
Log Out (http://jurnalnasional.ump.ac.id/index.php/JUITA/login/signOut)

Journal Content

Search

Search Scope

All

Search

Browse
By Issue (http://jurnalnasional.ump.ac.id/index.php/JUITA/issue/archive)
By Author (http://jurnalnasional.ump.ac.id/index.php/JUITA/search/authors)
By Title (http://jurnalnasional.ump.ac.id/index.php/JUITA/search/titles)
Other Journals (http://jurnalnasional.ump.ac.id/index.php/index)

Font Size

Information

For Readers (http://jurnalnasional.ump.ac.id/index.php/JUITA/information/readers)
For Authors (http://jurnalnasional.ump.ac.id/index.php/JUITA/information/authors)

Keywords

Android (http://jurnalnasional.ump.ac.id/index.php/JUITA/search?subject=Android) Aplikasi (http://jurnalnasional.ump.ac.id/index.php/JUITA/search?subject=Aplikasi) Augmented Reality (http://jurnalnasional.ump.ac.id/index.php/JUITA/search?subject=Augmented%20Reality) Beasiswa-PPA (http://jurnalnasional.ump.ac.id/index.php/JUITA/search?subject=Beasiswa-PPA) Forward Chaining (http://jurnalnasional.ump.ac.id/index.php/JUITA/search?subject=Forward%20Chaining) Fuzzy Quantification Theory I (http://jurnalnasional.ump.ac.id/index.php/JUITA/search?subject=Fuzzy%20Quantification%20Theory%20I) Mamdani (http://jurnalnasional.ump.ac.id/index.php/JUITA/search?subject=Mamdani) MySQL (http://jurnalnasional.ump.ac.id/index.php/JUITA/search?subject=MySQL) Rekayasa Perangkat Lunak (http://jurnalnasional.ump.ac.id/index.php/JUITA/search?subject=Rekayasa%20Perangkat%20Lunak) SMS Gateway (http://jurnalnasional.ump.ac.id/index.php/JUITA/search?subject=SMS%20Gateway) Sistem informasi (http://jurnalnasional.ump.ac.id/index.php/JUITA/search?subject=Sistem%20informasi) Tsukamoto (http://jurnalnasional.ump.ac.id/index.php/JUITA/search?subject=Tsukamoto) Web Service (http://jurnalnasional.ump.ac.id/index.php/JUITA/search?subject=Web%20Service) backpropagation (http://jurnalnasional.ump.ac.id/index.php/JUITA/search?subject=backpropagation) backward chaining (http://jurnalnasional.ump.ac.id/index.php/JUITA/search?subject=backward%20chaining) decision support system (http://jurnalnasional.ump.ac.id/index.php/JUITA/search?subject=decision%20support%20system) expert system (http://jurnalnasional.ump.ac.id/index.php/JUITA/search?subject=expert%20system) interest in learning (http://jurnalnasional.ump.ac.id/index.php/JUITA/search?subject=interest%20in%20learning) learning achievement (http://jurnalnasional.ump.ac.id/index.php/JUITA/search?subject=learning%20achievement) learning motivation (http://jurnalnasional.ump.ac.id/index.php/JUITA/search?subject=learning%20motivation) motivasi belajar (http://jurnalnasional.ump.ac.id/index.php/JUITA/search?subject=motivasi%20belajar)

JUITA : Jurnal Informatika e-ISSN: 2579-8901 p-ISSN: 2086-9398

(https://scholar.google.co.id/citations?user=l2ufArUAAAAJ&hl=en) (https://doaj.org/toc/2579-8901) (http://id.portalgaruda.org/?ref=browse&mod=viewjournal&journal=624) (http://sinta2.ristekdikti.go.id/journals/detail?id=1153) (https://search.crossref.org/?q=2579-8901)

(https://www.statcounter.com/)

(http://statcounter.com/p11268461/summary/?guest=1)

Assessment and Mitigation of Information Security Policy in Budgeting System for Charity Organization XYZ using KAMI Index 4.1

Tawar[1], Imam Riadi[2], Adiniah Gustika Pratiwi[3], Ariqah Adliana Siregar[4]

[1,2,3,4] *Universitas Ahmad Dahlan, Yogyakarta, Indonesia*

[1]tawar@is.uad.ac.id,
[2]imam.riadi@is.uad.ac.id,[3]adiniah1800016038@webmail.uad.ac.id,
[4]ariqah1800016036@webmail.uad.ac.id

Abstract - Threats to information resources require information security management policies in every agency. The Information Security Index (KAMI Index) is one of the methods developed by the Ministry of Communication and Information Technology, used to evaluate the maturity level, completeness of ISO/IEC 27001:2013 implementation and information security readyness. As a national zakat institution, XYZ Organization has utilized information technology in several systems, including the budgeting system. However, the information security index has never been measured. This condition may result in the risk of threats to information security, so it is necessary to measure. The Budgeting System needs to be measured using KAMI Index 4.1. The assessment criteria are carried out on seven categories to know how the quality of the information security policy is. The results of this assessment, XYZ organization gets an electronic system score is 17, governance 75, risk management 30, framework 31, asset management 37, ICT 38, securing third party involvement 40%, service security 20%, personal data protection 27% so the total score of 5 categories is 211 or at level I+ to II. This organization has started implement the framework at early stage and has not met the initial requirements for ISO/IEC 27001:2013 certification.

Keywords: Assessment, Information, KAMI Index, Security, zakat institution.

I. INTRODUCTION

The development of information technology (IT) every day is advancing very rapidly. Due to this development, the entire organization or company must adapt and implement IT advancements[1]. Charity Organization XYZ is one of the organizations that implement IT advances. This organization is a national-level zakat institution trusted to manage zakat funds, infaq, waqf, and other philanthropic funds, both individuals, institutions, companies, and other agencies. This agency is intended as a zakat management institution with modern management that can deliver zakat to be part of the social problem solver that continues to grow.

There are six pillars of the program run by Charity Organization XYZ, namely education, health, economy, social humanity, da'wah, and the environment. This Charity agency also has several selected donation programs, including zakat, infaq, programs, and qurban, but they don't accept any form of funds originating from crime.

Charity Organization XYZ has several systems in managing zakat funds, one of which is a budgeting system with the system has risks and gaps in information security. The system needs to analyze and evaluate the level of readiness (completeness and maturity) of its security implementation. The existence of a threat to these information resources requires the presence of an information security management in every agency, including government-owned public service providers[2]. Information security describes efforts to protect computers and non-computers, data facilities, and information from misuse by irresponsible people[3].

In the implementation of ICT governance, the information security factor is a crucial aspect to consider considering that the performance of ICT governance will be disrupted if information as one of the main objects of ICT governance experiences problems in the form of interference and threats concerning aspects of confidentiality,

integrity, and availability (availability). The Ministry of Communication and Information Technology of the Republic of Indonesia has issued regulation number 4 of 2016 concerning Information Security Management Systems (ISMS)[4]. As a form of implementation of the applicable law, the Ministry of Communication and Information (Kemkominfo) of the Republic of Indonesia expects organizations that operate electronic systems to carry out SNI ISO 27001 certification related to information security[5]. Several assessment tools can be used regarding information security in institutions, for example, by using ISO 27001:2013[6], COBIT[7], a combination of COBIT 4.1, ITIL v.3, and ISO 27001[8].

The National Standardization Agency was established on April 8, 2016, SNI ISO/IEC 27001:2013 as the national standard in information technology. To obtain a standardized measure of SNI ISO/IEC 27001:2003, the National Cyber and Crypto Agency (BSSN) issued an application that is used as a tool to analyze and evaluate the level of readiness (completeness and maturity) of the application of SNI ISO/IEC 27001:2003, namely the KAMI Index (Information Security Index)[9].

The Information Security Index (KAMI) is one of the methods developed by the Ministry of Communication and Informatics, used to evaluate the maturity level, the completeness of the implementation of ISO/IEC 27001:2013, and the readiness of information security[10]. The KAMI index is not intended to analyze the feasibility or effectiveness of existing forms of protection, but rather as a tool to provide an overview of the state of readiness of the information security framework to the leadership of corporate agencies[11] Thus, Charity Organization XYZ needs to apply the KAMI Index (Information Security) as a tool to analyze and evaluate the level of security readiness by the criteria in SNI ISO/IEC 27007.

A. Information Security

Information security is an effort to prevent fraud (*cheating*)[12] or detect fraud in information-based systems, where the information itself has no physical meaning Information security that exists today can become a necessity for an organization because security in knowledge is a fundamental problem in a business[13].

Information security is intended to maintain the Confidentiality aspect, Integrity, and Availability of information when accessed. Below is an image that describes the elements of information security[14].

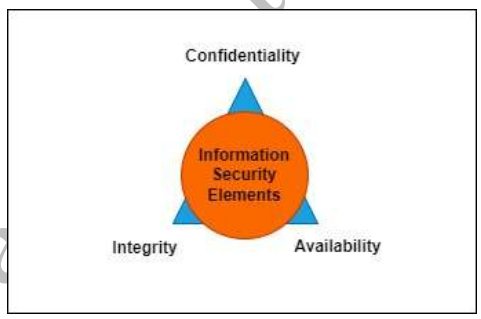


Fig. 1 Information Security Elements

Correlation between threats and vulnerabilities, namely weaknesses that exist in the system that these threats can exploit. Efforts to reduce the vulnerability aspects in the system can also reduce threats to the system[15] .

Several information security methods are used to minimize and manage risks to information security. These methods include Risk Assessment, Maturity Level to assess the level of information security that has been implemented by the organization and implement information security policies to regulate and manage information security.

B. Information Security Management Standard

Information Security Management Standard (ISMS) is a goal in achieving the goals of an organization by establishing, implementing, using, monitoring, reviewing, maintaining, and improving information security[16].

Standard ISO (International Organization for Standardization) or the International Standardization Organization has developed many standards on Information Security Management System (ISMS) since 2005 in requirements and guidelines. ISMS standard grouped as an ISO 27000 family or series consisting of:

1) ISO/IEC 27000:2009 – ISMS *Overview And Vocabulary*
2) ISO/IEC 27001:2005 – ISMS *Requirements*
3) ISO/IEC 27002:2005 – *Code of Practice for ISMS*
4) ISO/IEC 27003:2010 – ISMS *Implementation Guidance*
5) ISO/IEC 27004:2009 – ISMS *Measurements*
6) ISO/IEC 27005:2008 – *Information Security Risk Management*
7) ISO/IEC 27006: 2007 – ISMS *Certification Body Requirements*
8) ISO/IEC 27007 – *Guidelines for ISMS Auditing*

Judging from the ISO 27000 series standard above, up to September 2011, only ISO/IEC 27001:2005 has been adopted National Standardization Agency (BSN) as Indonesian National Standard (SNI) Indonesian language numbered SNI ISO/IEC 27001:2009[17].

C. ISO 27001

ISO 27001 is a standard intended to assist companies in protecting the security of company assets and protecting the Information Security Management System (ISMS). ISO 27001 is a standard issued by International Organization for Standardization[18]. ISO 27001 provides a framework for the scope of information technology and asset management in ensuring that the information security established within an organization is by SNI [19].

ISO 27001 has the advantage that the ISO 27001 standard is very flexible depending on the organization's needs[20]. The ISO 27001 standard is independent of information technology products, requires the use of a risk-based management approach, and is designed to ensure that the selected security controls can protect information assets from various risks and provide confidence in the level of security for interested parties[21]. The organizational structure in ISO 27001 is divide into 2, namely:

1) Clausul (*Mandatory prosess)*

The organization must meet requirements if implementing the ISMS (Information Security Management System).

2) Annex A (*security control)*

The reference document can be used to determine the security controls that need to be established in the ISMS (Information Security Management System)[22].

D. KAMI Index

KAMI Index is an evaluation tool to analyze an organization's information security level of readiness. This evaluation tool is not intended to explore the feasibility or effectiveness of existing forms of security but rather to provide an informative description of the state of readiness (completeness and maturity) of an organization's framework[23].

The form of evaluation applied by the Index is made so that it can be used by organizations of various levels, sizes, and levels of importance in using ICT in supporting the implementation of existing processes.

KAMI Index evaluation process can be used by organizations on a national scale and small. The evaluation process is carried out through many questions in each of the areas below:

1) Category of Electronic System used by Agencies
2) Information security governance category
3) Information Security Risk Management
4) Information Security Framework
5) Asset management category
6) Information Technology and Security

7) Suplement: Evaluation area for aspects of Third Party Engagement Security, Cloud Service Security and personal data protection.

The initial stage before the quantitative assessment process is carried out is to carry out a classification process for the Electronic Systems used with the aim of grouping the Electronic Systems used into certain "levels": Low, High, Strategic.

TABLE I
ELECTRONIC SYSTEM CATEGORY MATRIX

ELECTRONIC SYSTEM CATEGORY				
Low		**Final Score**		**Readiness Status**
10	15	0	174	Not Feasible
		175	312	Fulfillment of the basic framework
		313	535	Pretty good
		536	645	Good
High		**Final Score**		**Readiness Status**
16	34	0	272	Not Feasible
		273	455	Fulfillment of the basic framework
		456	583	Pretty good
		584	645	Good
Strategic		**Final Score**		**Readiness Status**
35	50	0	333	Not Feasible
		334	535	Fulfillment of the basic framework
		536	609	Pretty good
		610	645	Good

Based on TABLE I, the Electronic System category matrix shows the final score, which will be adjusted to the readiness status of the Agency or Organization for information security.

The evaluation process in each area of KAMI Index discusses aspects in achieving the primary goal of securing the site. The form of security using minimum readiness is required for the SNI ISO/IEC 27001:2013 standard certification process. The following is a score mapping table for self-assessment and forms a matrix between security category statuses[24].

TABLE II
KAMI INDEX SECURITY CATEGORY

	Security Category		
Security Status	**1**	**2**	**3**
Not done	0	0	0
In planning	1	2	3
In progress	2	4	6
Fully applied	3	6	9

In TABLE II, the evaluation process respondents are asked to provide responses starting from areas related to the form:

1) Label 1: Information Security Basic Framework
2) Label 2: Effectiveness and Consistency of Its Application
3) Label 3: Ability to Improve Information Security Performance [25].

The next grouping is based on the maturity level of the security application, which refers to the maturity level used by the COBIT or CMMI framework. The maturity level will be used to report the mapping and ranking of information security readiness in the Organization.

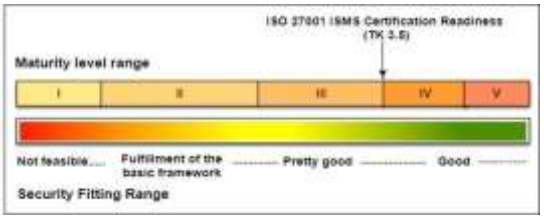


Fig. 2 Completeness and Maturity Level

Based on Fig. 2, the maturity level is defined as:

1) Level I - Initial Condition
2) Level II - Implementation of the Basic Framework
3) Level III - Defined and Consistent
4) Level IV - Managed and Scalable
5) Level V - Optimal

The above maturity levels are added with levels between I+, II+, III+, and IV+, so there are nine levels of maturity in total. Based on the ISO/IEC 27001:2013 standard, the expected maturity level as the minimum certification threshold is Level III+.

II. METHOD

This research assesses the level of information security in an organization using KAMI Index 4.1 method. Fig. 3 depicts the research flow and the following explanation:

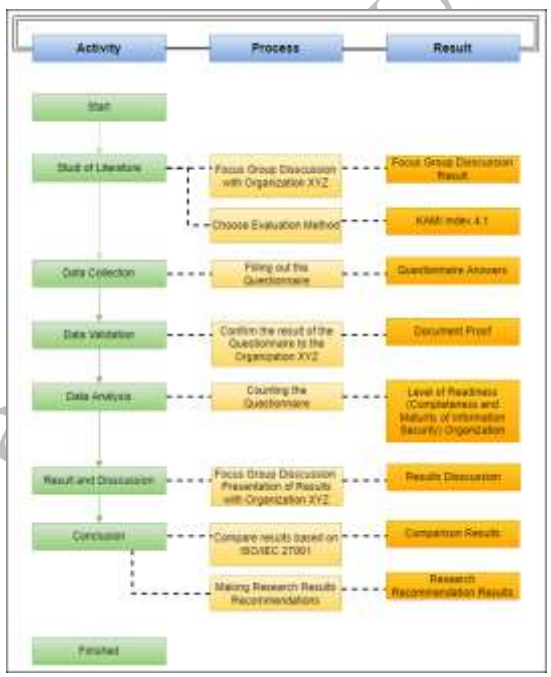


Fig. 3 Research Methodology

The methodology is the stage or flow used in conducting research. In this research, several steps were carried out, namely:

1) Literatures Study

FGD (Focus Group Discussion) with Organization XYZ is the initial process in the literature study. The FGD was conducted to find out the problems regarding the existing system and what method would be used in this research.

After getting the results from the FGD, the next step is to determine or choose what method can solve the problems. The literature study was carried out by reviewing previous research which was relevant to the research to be carried out and then selecting the KAMI Index 4.1 method according to the ISO/IEC 27001 standard to solve the problems found.

2) Data Collection

The next stage is to collect data by filling out the KAMI Index questionnaire conducted by selected respondents (responsible IT staff & and other related staff) according to the questionnaire category. Questionnaire KAMI Index, which is used in the latest version of 4.1.

3) Data Validation

The next stage is data validation by confirming to the respondents to ensure the data provided is in its original state. Confirmation of this data is done by online meeting using Zoom Meeting application with respondents and asks for evidence in related documents (if any) in each area.

4) Data Analysis

Data analysis is a step for calculating the questionnaire results and analyzing the level of readiness (completeness and maturity) of information security in the budgeting system.

5) Result and Disscussion

The next stage is presenting the results by conducting an FGD with Organization XYZ

6) Conclusion

The last stage is concluding the results of the research conducted. These results are then compared with the control in ISO 27001. After that, the following process is the recommendation process to provide input on deficiencies that the agency has not carried out.

III. RESULTS AND DISCUSSION

The results of the evaluation of the level of readiness (completeness and maturity) of information security in the budgeting system are grouped into seven category areas according to KAMI Index version 4.1. These categories include Electronic Systems, Information Security Governance, Information Security Risk Management, Information Security Management Framework, Information Asset Management, Information Technology, and Security and Supplements. The evaluation results from the seven categories are shown in the dashboard KAMI Index in Fig. 4.

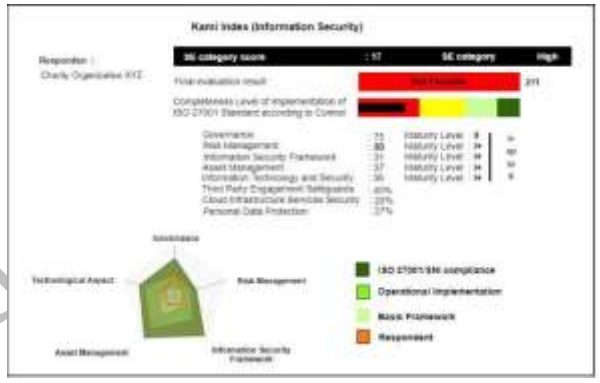


Fig. 4 Dashboard KAMI Index 4.1

1. Electronic System Category

The electronic system category is the first category in the evaluation. The electronic system category evaluates the importance of using electronic systems in the budgeting system. The results of the assessment of the importance of the use of Electronic Systems in the budgeting system get score of 17, so that it can be included in the "High" category according to the guide table for the assessment of the electronic system category in TABLE I. the "High" category ranges from a score of 16 to 34. The total score for the electronic system category on the budgeting system can be seen in the dashboard of the KAMI Index 4.1 in Fig. 4.

2. Information Security Governance Category

The category of information security governance is an evaluation that can affect data on the budgeting system. Assessment of Information Security Governance in the budgeting system at Organization XYZ obtained a total evaluation score at 75 out of 22 questions with maturity level II status (Implementation of the basic framework). The expected maturity level for the minimum threshold for certification readiness is Level III+. Still, the results of

Information Security Governance are only at maturity level II, which means that they are already implementing the basic framework. The evaluation results of information security governance are shown in TABLE III.

TABLE III
INFORMATION SECURITY GOVERNANCE EVALUATION RESULTS

Security Status	**Maturity Level**						**Total**
	1	**score**	**2**	**score**	**3**	**score**	
Not done	0	0	0	0	0	0	0
In Planning	1	0	2	0	3	0	0
In progress	2	10	4	20	6	18	48
Fully applied	3	9	6	18	9	0	27
Total Score							**75**

3. Information Security Risk Management Category

The information security risk category evaluates the management of information security risk, including various risks that can occur and affect information data on the budgeting system. Assessment of Information Security Risk Management on the budgeting system obtained a total evaluation value at score 30 out of 16 questions with maturity level status I+ (Initial Condition). The expected maturity level for the minimum certification readiness threshold is Level III+. However, this results are only at maturity level I+. The evaluation results are shown in TABLE IV.

TABLE IV
INFORMATION SECURITY RISK MANAGEMENT EVALUATION RESULTS

Security Status	**Maturity Level**						**Total**
	1	**score**	**2**	**score**	**3**	**score**	
Not done	0	0	0	0	0	0	0
In Planning	1	2	2	2	3	0	4
In progress	2	16	4	4	6	0	20
Fully applied	3	0	6	6	9	0	6
Total Score							**30**

4. Information Security Framework Category

Assessment of the Information Security Framework on the budgeting system obtained a total evaluation value of the Information Security Framework at score 31 out of 29 questions with a maturity level status of I+ (Initial Condition). The expected maturity level for the minimum certification readiness threshold is Level III+. However, the Information Security Framework results are only at maturity level I+. The evaluation results are shown in TABLE V.

TABLE V
INFORMATION SECURITY FRAMEWORK EVALUATION RESULTS

Security Status	**Maturity Level**						**Total**
	1	**score**	**2**	**score**	**3**	**score**	
Not done	0	0	0	0	0	0	0
In Planning	1	4	2	6	3	0	10
In progress	2	4	4	8	6	0	12
Fully applied	3	9	6	0	9	0	9
Total Score							**31**

5. Asset Management Category

Assessment of Information Security Asset Management on the budgeting system at Organization XYZ obtained an evaluation of Information Security Asset Management of 37 out of 38 questions with maturity level status I+ (Initial Condition). The expected maturity level for the minimum certification readiness threshold is Level III+. However, the Information Security Asset Management result is only at maturity level I+. The evaluation results of information security governance are shown in TABLE VI.

TABLE VI
ASSET MANAGEMENT EVALUATION RESULTS

Security Status	**Maturity Level**						**Total**
	1	**score**	**2**	**score**	**3**	**score**	
Not done	0	0	0	0	0	0	0
In Planning	1	6	2	2	3	0	8
In progress	2	14	4	12	6	0	26
Fully applied	3	3	6	0	9	0	3
Total Score							**37**

6. Category Information Technology and Security

Assessment of Information Security Technology Aspects on the budgeting system obtained score at 38 out of 26 questions, with maturity level status I+ (Initial Condition). The evaluation results of information security governance are shown in TABLE VII.

TABLE VII
THE RESULTS OF THE EVALUATION OF TECHNOLOGY AND INFORMATION SECURITY

Security Status	**Maturity Level**						**Total**
	1	**score**	**2**	**score**	**3**	**score**	
Not done	0	0	0	0	0	0	0
In Planning	1	1	2	0	3	0	1
In progress	2	14	4	8	6	0	22
Fully applied	3	3	6	12	9	0	15
Total Score							**38**

7. Supplement Category

The evaluation results at the supplement stage obtained that the maturity level for securing third-party involvement was 40%. Then for the security of cloud infrastructure services by 20% and the last is personal data protection by 27%.

IV. CONCLUSION

Based on the results of the evaluation conducted on the level of readiness (completeness and maturity) of information security by using KAMI Index on the budgeting system in Organization XYZ, it can be concluded that: The Electronic System Area got a score of 17, so it was included in the high category; From the five observed information security areas, it is seen that they have better governance aspects compared to other information security areas (close to certification standards); Framework Area (31<36), Asset Management Area (37<72), and Technology Aspect Area (38<42), giving the results do not meet the basic framework. So, they have to improve somo aspect of information security policy; Of the five information security areas (Information Security Governance, Information

Security Risk Management, Information Security Framework, Asset Management, and Technology), a total score of 211 is obtained. Based on the correlation with the Electronic System Category in TABLE I, 211 is between 0-272. Based on Fig 2, the level of completeness of information system security has a readiness status of "Not Feasible."; The minimum limit that must be achieved to be able to carry out ISO 27001 certification is III+. For now, the maturity level of the Work Unit of the Central XYZ Organization in the budgeting system is only limited to I+ to II. The information system security level is at the level of "Implementation of the Basic Framework."

ACKNOWLEDGEMENT

Thank you to Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) Universitas Ahmad Dahlan who have provided funding for this research activity through Skema Penelitian Unggulan Program Studi (PUPS) in 2021 based on contract number PUPS-278/SP3/LPPM-UAD/VI/2021.

REFERENCES

[1] E. R. Pratama, Suprapto, dan A. R. Perdanakusuma, "Evaluation of Information Technology Security System Governance Using the KAMI Index and ISO 27001: A Case Study of KOMINFO East Java Province," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 11, hal. 5911–5920, 2018, [Daring]. Tersedia pada: http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/3465.

[2] T. Effendy *et al.*, "Evaluation of Information Security Using the Information Security Index (US) at the Regional Office of the Ministry of Law and Human Rights Diy," vol. 3, no. 1, hal. 1–6, 2020.

[3] B. Sutara, "PDAM Titra Medal Information Security Measurement Using the US Index for Information Security Maturity Level Analysis," vol. 17, no. 2, hal. 34–41, 2018, [Daring]. Tersedia pada: https://ejournal.ikmi.ac.id/index.php/jict-ikmi/article/view/32.

[4] Yustanti, W. Rahadian, B. Anita, Q. Prihanto, dan Agus, "Analysis Of Readiness And Maturity Level Of Implementation Of Iso 27001: 2013 Using Information Security Index 3: 2015 At Upt . Ppti State University Surabaya The Ministry of Communication and Information Technology of the Republic of Indonesia has issued regulation number," *Inform. P. T., Inform. J. T., Surabaya, U. N., Hari, D., Bulan, T., Hari, D., Bulan, T. (2016). Anal. Tingkat Kesiapan Dan Kematangan Implementasi Iso 27001 2013 Menggunakan Indeks Keamanan Inf. 3 2015 Pada Upt . Ppti Univ. N*, no. 4, hal. 1602–1613, 2016.

[5] M. R. Slamet, F. Wulandari, dan D. Amalia, "Assessment of Technology Security in Electronic Learning Systems Using the Information Security Index at Batam State Polytechnic," *J. Appl. Bus. Adm.*, vol. 3, no. 1, hal. 162–171, 2019, doi: 10.30871/jaba.v3i1.1305.

[6] W. W. W. S. Haries Anom Suseyto Aji Nugroho, "The syllogism method and for the validity of the answers from respondents in the analysis of the Maturity Level of Information Security Based on Sni Iso 27001:2013 at the Department of Population and Civil Registration of the City of Xyz," *J. Transform.*, vol. 14, no. 2, 2019.

[7] J. F. Andry dan A. K. Setiawan, "It Governance Evaluation Using Cobit 5 Framework on the National Library," *J. Sist. Inf.*, vol. 15, no. 1, hal. 10–17, 2019, doi: 10.21609/jsi.v15i1.790.

[8] Y. Sekhara, H. Medromi, dan H. Nahla, "Multi Agent Decision system for the IT Governance Platform," vol. 15, no. 5, hal. 290–306, 2017.

[9] A. R. Riswaya, A. Sasongko, dan A. Maulana, "Evaluation of Information Technology Security Governance Using Our Index for Preparation of Sni Iso/Iec 27001 Standard (Case Study: Stmik Mardira Indonesia)," *J. Comput. Bisnis, Vol. 14, No. 1, Juni 2020, 10-18 ISSN 1978-9629, ISSN 2442-4943*, vol. 14, no. 1, hal. 10–18, 2020.

[10] N. A. Widodo dan and A. F. R. , R. Rizal Isnanto, "Information Security Management System Planning And Implementation Based On Iso/Iec 27001:2005 StandardS (Case Study in a National Private Bank)," vol. 4, no. 1, hal. 60–66, 2016.

[11] N. E. Wowor *et al.*, "AAnalysis of Manado City Government Information Security Using Our Index," *J. Tek. Inform.*, vol. 13, no. 3, hal. 1–10, 2018, doi: 10.35793/jti.13.3.2018.28081.

[12] T. Hartati, "Information Security Management System Planning in Academic Field Using ISO 27001: 2013," *KOPERTIP J. Ilm. Manaj. Inform. dan Komput.*, vol. 1, no. 2, hal. 63–70, 2017, doi: 10.32485/kopertip.v1i02.24.

[13] F. Febrianto dan D. I. Sensuse, "Evaluation of information security using ISO / IEC 27002: a case study on the Banjarnegara Tunas Bangsa," *Infokam*, vol. 2, no. 2013, hal. 21–27, 2017.

[14] R. C. Annisyah, A. Budiono, dan R. Fauzi, "Analysis And Design Of Information Security Management Directorate Of Information Systems Of Telkom University Using The Information Security Index (Kami) In The Area Of Information Asset Management, Technology And Information Security" vol. 8, no. 2, hal. 2663–2677, 2021.

[15] N. Matondang, I. N. Isnainiyah, dan A. Muliawatic, "Analysis of Information System Data Security Risk Management (Case Study: XYZ Hospital)," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 2, no. 1, hal. 282–287, 2018, doi: 10.29207/resti.v2i1.96.

[16] W. Apriandari dan A. Sasongko, "Information Security Management System Analysis Using Sni Iso / Iec 27001: 2013 in the Regional Government of Sukabumi City (Case Study: At Diskominfo Sukabumi City)," *Ilm. SANTIKA*, vol. 8, no. 1, hal. 715–729, 2018.

[17] R. Adi, P. Pratama, R. Sengkey, dan C. Punusingon, "Information Security Analysis of Southeast Minahasa District Government Using KAMI Index," vol. 15, no. 3, hal. 189–198, 2020.

[18] B. A. Firzah, "Evaluation of Information Security Management Using the Information Security Index (US) Based on Iso / Iec 27001: 2013 at the Directorate of Information Technology and System Development (Dptsi) Its Surabaya Evaluating Information Security Management Using KAMI Index," vol. 6, no. 1, 2017.

[19] H. Hambali dan P. Musa, "Analysis of Governance Security Management Information System Using Index Kami in Central Government Institution," *Angkasa J. Ilm. Bid. Teknol.*, vol. 12, no. 1, 2020, doi: 10.28989/angkasa.v12i1.563.

[20] M. Bakri dan N. Irmayana, "Analysis and Implementation of Simhp Bpkp Information Security Management System Using ISO 27001 Standard," *J. Tekno Kompak*, vol. 11, no. 2, hal. 41, 2017, doi: 10.33365/jtk.v11i2.162.

[21] M. Lenawati, W. W. Winarno, dan A. Amborowati, "Information Security Governance in PDAM Using ISO/IEC 27001:2013 and COBIT 5," *Sentra Penelit. Eng. dan Edukasi*, vol. 9, no. 1, hal. 44–49, 2017, [Daring]. Tersedia pada: http://speed.web.id/jurnal/index.php/speed/article/view/220.

[22] Y. C. Pradipta, Y. Rahardja, M. N. N. Sitokdana, U. Kristen, dan S. Wacana, "Information and Communication Technology of Aviation and Space (Pustikpan) Using Sni Iso / Iec 27001: 2013," hal. 352–358, 2013.

[23] W. C. Pamungkas dan F. T. Saputra, "Evaluation of Information Security at SMA N 1 Sentolo Based on Information Security Index (KAMI) ISO/IEC 27001:2013," *J. Sist. Komput. dan Inform.*, vol. 1, no. 2, hal. 101, 2020, doi: 10.30865/json.v1i2.1924.

[24] D. A. Wati, A. Budiono, dan R. Fauzsi, "Analysis And Design Of Information Security Management In The Directorate Of Telkom University Information Systems With Information Security Index (Us) In Security Governance Area Of Information, Risk Management Of Information Security And Information Framework For Information Security Management," *Αγαη*, vol. 8, no. 5, hal. 55, 2019.

[25] BSSN, "Information Security Index (KAMI Index)," *Badan Siber dan Sandi Negara*, no. November, 2019.